ETSI GR NFV-IFA 037 V4.1.1 (2021-12)

Network Functions Virtualisation (NFV) Release 4; Architectural Framework; Report on further NFV support for 5G

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/NFV-IFA037

Keywords
5G, architecture, management, NFV

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document assesses the 5G network capabilities and features, and it determines how NFV can be utilized to support the implementation and deployment of such networks by profiling current NFV architectural framework capabilities and features. Where applicable, the present document also provides recommendations for enhancements to the NFV architectural framework and its functionality aiming to provide further support to address 5G network characteristics.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] ETSI TS 123 501 (V16.9.0): "5G; System Architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.9.0 Release 16)".

[i.3] ETSI TS 128 533 (V16.7.0): "5G; Management and orchestration; Architecture framework (3GPP TS 28.533 version 16.7.0 Release 16)".

[i.4] ETSI TS 138 300 (V16.6.0): "5G; NR; NR and NG-RAN Overall description; Stage-2 (3GPP TS 38.300 version 16.6.0 Release 16)".

[i.5] ETSI TS 128 530 (V16.4.0): "5G; Management and orchestration; Concepts, use cases and requirements (3GPP TS 28.530 version 16.4.0 Release 16)".

[i.6] ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Functional requirements specification".

[i.7] ETSI GR NFV-IFA 024: "Network Functions Virtualisation (NFV) Release 3; Information Modeling; Report on External Touchpoints related to NFV Information Model".

[i.8] ETSI TS 123 502 (V16.9.0): "5G; Procedures for the 5G System (5GS) (3GPP TS 23.502 version 16.9.0 Release 16)".

[i.9] ETSI GS NFV-IFA 014: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Network Service Templates Specification".

[i.10] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

[i.11] ETSI GS NFV-SOL 001: "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; NFV descriptors based on TOSCA specification".

[i.12] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; VNF Descriptor and Packaging Specification".

[i.13] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.14] ETSI TS 133 501 (V16.6.0): "5G; Security architecture and procedures for 5G system (3GPP TS 33.501 version 16.6.0 Release 16)".

[i.15] Void.

[i.16] ETSI GR NFV-IFA 029: "Network Functions Virtualisation (NFV) Release 3; Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS".

[i.17] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

NOTE: Available from https://tools.ietf.org/html/rfc6749.

[i.18] ETSI GS NFV-IFA 008: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[i.19] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[i.20] ETSI TS 133 210 (V16.4.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 16.4.0 Release 16)".

[i.21] ETSI TS 133 310 (V16.7.0): "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310 version 16.7.0 Release 16)".

[i.22] ETSI TS 123 682 (V16.9.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements to facilitate communications with packet data networks and applications (3GPP TS 23.682 version 16.9.0 Release 16)".

[i.23] ETSI TS 123 222 (V16.9.0): "LTE; 5G; Common API Framework for 3GPP Northbound APIs (3GPP TS 23.222 version 16.9.0 Release 16)".

[i.24] ETSI TS 129 522 (V16.7.0): "5G; 5G System; Network Exposure Function Northbound APIs; Stage 3 (3GPP TS 29.522 version 16.7.0 Release 16)".

[i.25] ETSI TS 123 503 (V16.8.0): "5G; Policy and charging control framework for the 5G System (5GS); Stage 2 (3GPP TS 23.503 version 16.8.0 Release 16)".

[i.26] ETSI TS 123 288 (V16.7.0): "5G; Architecture enhancements for 5G System (5GS) to support network data analytics services (3GPP TS 23.288 version 16.7.0 Release 16)".

[i.27] ETSI GS NFV-IFA 030: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Multiple Administrative Domain Aspect Interfaces Specification".

[i.28] WBA and NGMN Alliance: "RAN Convergence Paper", 2019.

[i.29] ETSI TS 123 316 (V16.6.0): "5G; Wireless and wireline convergence access support for the 5G System (5GS) (3GPP TS 23.316 version 16.6.0 Release 16)".

[i.30] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[i.31] ETSI GS NFV-IFA 040: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification".

[i.32] ETSI GS NFV-SOL 006: "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; NFV descriptors based on YANG Specification".

[i.33] ETSI TS 129 510 (V16.7.0): "5G; 5G System; Network Function Repository Services; Stage 3 (3GPP TS 29.510 version 16.7.0 Release 16)".

[i.34] ETSI GR NFV-SEC 005: "Network Functions Virtualisation (NFV); Trust; Report on Certificate Management".

[i.35] ETSI TS 124 502 (V16.7.0): "5G; Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP access networks (3GPP TS 24.502 version 16.7.0 Release 16)".

[i.36] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

[i.37] IETF RFC 4303: "IP Encapsulation Security Payload (ESP)".

NOTE: Available from https://tools.ietf.org/html/rfc4303.

[i.38] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

NOTE: Available from https://tools.ietf.org/html/rfc7296.

[i.39] ETSI TS 128 531 (V16.9.0): "5G; Management and orchestration; Provisioning (3GPP TS 28.531 version 16.9.0 Release 16)".

[i.40] 3GPP TR 23.742: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Enhancements to the Service-Based Architecture (Release 16)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR NFV 003 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.1] and the following apply:

5GS	5G System
5G-CN	5G Core Network
5G-VN	5G Local Area Network
ACL	Access Control List
AMF	Access and mobility Management Function
AF	Application Function
AN	Access Network
AS	Application Server
ATSSS	Access Traffic Steering, Switching and Splitting
CA	Certificate Authority
CAPIF	Common API Framework
CN	Core Network
DB	DataBase
DN	Data Network
DNAI	DN Access Identifier
eMBB	enhanced Mobile Broadband
EPC	Evolved Packet Core
EST	Enrolment over Secure Transport
FQDN	Fully Qualified Domain Name

IPUPS	Inter-PLMN UP Security
MIoT	Massive Internet of Things
MO	Mobile Originated
MT	Mobile Terminated
N3IWF	Non-3GPP Interworking Function
NAS	Non Access Stratum
NEF	Network Exposure Function
NIDD	Non-IP Data Delivery
NRF	Network Repository Function
NWDAF	Network Data Analytics Function
PCF	Policy Control Function
PFD	Packet Flow Description
PLMN	Public Land Mobile Network
PDU	Protocol Data Unit
RAN	Radio Access Network
SBA	Service-Based Architecture
SCEF	Service Capability Exposure Function
SCP	Service Communication Proxy
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
SST	Slice/Service Type
TNGF	Trusted Non-3GPP Access Network Gateway Function
UDM	Unified Data Management
UDR	Unified Data Repository
UDSF	Unstructure Data Storage Function
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra Reliable and Low Latency Communications
V2X	Vehicle to Everything
W-5GAN	Wireline 5G Access Network
W-AGF	Wireline Access Gateway Function

4 Introduction and overview

4.1 Introduction to 5G network

The fifth generation of mobile network, or 5G system, is defined by 3GPP as the system consisting of 5G Access Network (AN), 5G Core Network (CN) and User Equipment (UE). The access network can be comprised of Next Generation Radio Access Network (NG-RAN) and/or non-3GPP AN. The 5G System architecture is specified in the ETSI TS 123 501 [i.2]. In addition, from a management perspective, the management and orchestration architecture framework of 5G system is specified in ETSI TS 128 533 [i.3].

As described in the ETSI TS 123 501 [i.2], the 5G System is defined to support data connectivity and services enabling deployments using techniques such as Network Functions Virtualisation (NFV) and Software Defined Networking (SDN). Thus, NFV is expected to play a key role in the realization and deployment of 5G networks.

In the present document, different characteristics of the 5G networks are introduced. From the list of characteristics, a set of key aspects related to the realization and deployment of 5G network are derived, which are further analysed to determine and profile the NFV features and aspects associated to them.

4.2 Characteristics of the 5G network

As described in the ETSI TS 123 501 [i.2], the 5G system, and in particular the control plane, is designed as a service-based architecture. The referred specification also lists key principles defining the characteristics of the 5G system, which are summarized hereafter:

- Network function modularization.

- Service-based interfaces, communication and service mesh.
- Network slicing.
- Convergent (3GPP and non-3GPP) access.
- Unified authentication framework.
- Stateless NF, with separation of data processing from state.
- Network capabilities exposure.
- Distribution of services across the network (local and centralized).
- Roaming capabilities.

From an NFV perspective, various capabilities, features and artefacts can be utilized to realize 5G system, such as:

- VNF componentization, and design of NS including VNF and PNF.
- Exposure of connectivity endpoints (as SAP).
- NFV descriptors and other design time constructs.
- Lifecycle management of VNF and NS.
- Assurance and monitoring of virtualised resources, VNF and NS.
- Management of diverse types of virtualised resource (compute, network and storage).
- Adoption of multiple virtualisation technologies, such as VM-based and container-based.
- Multi-tenancy, resource clusters and virtualised resource groups.

Only subsets of NFV capabilities, features and artefacts might be relevant to a specific 5G system characteristic. Further details are provided in clause 5, wherein the above introduced 5G system characteristics are analysed from the NFV's capabilities perspective to identify how the NFV can be utilized to realize and deploy the 5G system.

5 NFV support for 5G

5.1 Overview

Clause 5 performs the analysis and profiling of NFV features and capabilities to support 5G network characteristics. Each subsequent clause analyses, profiles and identifies gaps, where applicable, of a specific 5G network characteristic. 3GPP Release 16 documentation is used and referred (see clause 2) as the baseline for the 5G network characteristics evaluation and profiling.

The set of 5G network characteristics evaluated in the present document are:

- Characteristic #1: network function modularization, documented in clause 5.2.
- Characteristic #2: service-based interfaces, communication and service mesh, documented in clause 5.3.
- Characteristic #3: network slicing, documented in clause 5.4.
- Characteristic #4: distribution of services across the network, documented in clause 5.5.
- Characteristic #5: unified authentication framework, documented in clause 5.6.
- Characteristic #6: stateless NF, with separation of data processing from state, documented in clause 5.7.
- Characteristic #7: network capabilities exposure, documented in clause 5.8.

- Characteristic #8: roaming, documented in clause 5.9.
- Characteristic #9: convergent (3GPP and non-3GPP) access, documented in clause 5.10.

5.2 Characteristic #1: Network function modularization

5.2.1 Introduction

ETSI TS 123 501 [i.2] specifies the set of Network Functions (NFs) and entities that comprise the 5G system architecture. The same specification also introduces relevant support of 5GC for virtualised deployment scenarios, including (but not limited to) (refer to clause 5.21 of ETSI TS 123 501 [i.2]):

- An NF instance can be deployed as distributed, redundant, stateless, and scalable NF instance providing services from several location and several execution instances in each location.
- An NF instance can be deployed such that several NF instances are present within an NF set, providing distributed, redundant, stateless and scalability together as a set of NF instances.
- Other network entities that are not 3GPP NFs, such as SEPP and SCP, providing services to 3GPP NFs, can also be deployed distributed, redundant, stateless, and scalable.

The modularization of 3GPP NFs and 3GPP network entities is a key aspect of the 5G system which enables flexible and efficient deployment of the network to address specific service requirements, e.g. in the form of network slices. An NF can produce one or more service-based interface. Each service-based interface is exposed by a defined NF Service. The ETSI TS 123 501 [i.2] neither specifies interactions between NF services within one NF, nor determines how the NF modularization can be realized.

5.2.2 Profiling of related NFV capabilities, features and specifications

5.2.2.1 General NFV concepts

The NFV information and data modelling provides the following capabilities to support the modularization of NF using VNF and NS constructs:

- VNF componentization: a VNF can be comprised of one or more VNFC. A defined VNFC or set of VNFC can deliver and expose a specific service-related functionality.
- The deployment and lifecycle of a VNFC of a VNF is performed by NFV-MANO according to the resource requirements, workflows and information in the VNFD. A VDU in a VNFD represents the information and resource requirements descriptors used for deploying the resources realizing a VNFC. A VNFD can define one or more VNF deployment flavours. A VNF deployment flavour references specific VLDs and VDUs that are used to realize the deployment.
- NS composition: A set of VNF can be in turn compiled into a higher layer of abstraction, the Network Service (NS). As a result, VNFs become constituents of the NS.
- The deployment and lifecycle of an NS is performed by NFV-MANO according to the resource requirements, workflows and information in the NSD. An NSD can define one or more NS deployment flavours, wherein different NS deployment flavours reference specific NS VLDs, VNFDs, PNFDs and nested NSDs that are used to realize the deployment.

5.2.2.2 Specific profiling aspects and specification references

Concerning the modularization of a VNF and its scaling capabilities, ETSI GS NFV-IFA 011 [i.12] specifies the concept of "scaling aspects". A scaling aspect defines what components of a VNF can be scaled horizontally (i.e. scaling out and in) and their respective ranges. A scaling aspect associates sets of VNFC instances based on particular VDUs that are created or removed as part of the scaling. Scaling of VLs and Virtual IP addresses is also specified as part of the scaling deltas. At the interface level, the NFVO and EM can request the VNFM (via the VNF LCM interface) to scale a VNF on a particular scaling aspect, as specified in ETSI GS NFV-IFA 007 [i.13] and ETSI GS NFV-IFA 008 [i.18], respectively.

5.2.3 Potential solutions

5.2.3.1 Solution #1A: VNF realizes a specified 5G system NF

In this solution, a VNF realizes a specific 5G system NF. This solution leverages the VNF construct to support NF modularization. An NF exposing a set of NF Services can be realized as a VNF comprising different VNFCs. Hence, the set of NF Services that the NF produces are realized by providing corresponding VNFCs.

NOTE: The mapping between NF services and VNFCs can be one-to-one but other options are possible as well, e.g. an NF service can map to a specific VNF scaling aspect.

An NF can be deployed to offer one or a set of NF Services by defining different VNF deployment flavours in the VNF Package and its contained VNFD. The network operator can request instantiating a specific VNF deployment flavour that it knows will deliver the desired set of NF services.

Regarding the scaling of individual NF Services produced by the NF, since the NF Services can be associated to specific VNFC that realize the corresponding functionality, respective scaling aspects associated to such VNFC will enable scaling respective NF Services capacity.

5.2.3.2 Solution #1B: VNF realizes a specified 5G system NF service

In this solution, a VNF realizes a specific 5G system NF Service. This solution leverages the NS construct to support NF modularization. To assemble an NF, the network operator can compile the set of required NF Services by putting the corresponding VNFs as constituents of an NS. This approach has the advantage that it offers the possibility for individual deployment and upgrade/update of the NF Services. If needed the NSD used to assemble the NF Services can contain information about version dependencies between the NF Services.

The NSD deployment flavours can be used to provide the selection of the component NF services for the different deployment options.

The NS can be further referred as a nested NS into another NS to assemble a "higher-layer" NS mapping to a broader functional scope of the 5G network.

5.2.3.3 Solution #1C: VNF realizes multiple NFs

In this solution, a VNF realizes multiple 5G system NFs. 3GPP TR 23.742 [i.40] provides a number of examples of such a solution.

NOTE: The mapping between NFs and VNFCs can be one-to-one but other options are possible as well, e.g. an NF can map to a specific VNF scaling aspect.

A VNF can be deployed to provide the functionality of one or a set of NF by defining different VNF deployment flavours in the VNF Package and its contained VNFD. The network operator can request instantiating a specific VNF deployment flavour that it knows will deliver the desired set of NFs.

Scaling of individual VNFs is facilitated if the VNFD design is such that an NF naps to a scaling aspect.

5.2.4 Gap analysis

The referred ETSI NFV specifications in the present characteristic profiling do not document:

Gap #1.1: How the relationship between scaling aspects and NF Services can be known by the network operator or the consumer of the VNF LCM interface. This is particularly relevant in the case of Solution #1A, since a single VNF can produce more than one NF Service, even though NFV-MANO is not aware of the services that the deployed NS and VNF offer. However, the relationship can be specified in a non-MANO artefact within the VNF package.

Gap #1.2: The onboarding of an NSD is not permitted by the NFVO if all the VNF packages referenced in the NSD have not been onboarded. In the case where a subset of the NF Services is chosen for the deployment of a 3GPP NF, then only the respective VNF packages are delivered to the service provider and are onboarded. The NSD deployment flavour used for NS instantiation would include the respective subset of VNFs corresponding to the selected NF Services. The current NFVO behaviour can be relaxed to allow successful onboarding of an NSD even if not all VNF packages have been previously onboarded. The same principle applies for the nested NSDs and PNFDs used in the NSD.

Gap #1.3: Information in the NSD about any version dependencies between VNFs that need to be observed at the time of software upgrades.

5.3 Characteristic #2: Service-based interfaces, communication and service mesh

5.3.1 Introduction

ETSI TS 123 501 [i.2] specifies the 5G system, whose 5G architecture is defined as service-based, yet the interactions between Network Functions (NFs) are still represented in two ways:

a) a service-based representation, where network functions within the control plane enable other authorized network functions to access their services; and

b) a reference point representation, where interactions exist between the NF services in the network functions on a point-to-point basis between any two network functions.

In either case, network functions within the 5GC control plane use only service-based interfaces for their interactions.

Figure 5.3.1-1 depicts the non-roaming reference architecture of 5G system in service-based form. ETSI TS 123 501 [i.2] also provides equivalent representations of the 5G System in the reference point form.

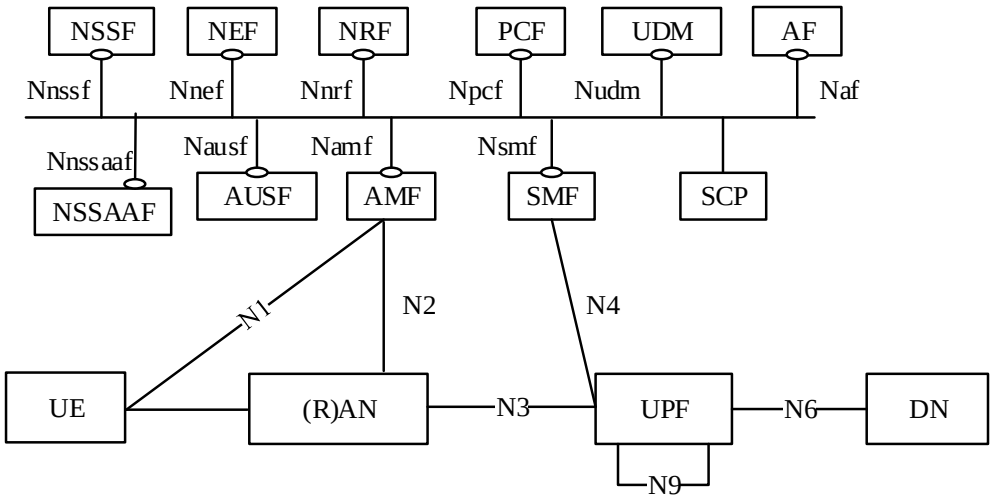


Figure 5.3.1-1: Non-roaming 5G System architecture (from ETSI TS 123 501 [i.2])

The set of NF of the 5G System exhibit (expose) service-based interfaces. For instance, the Access and Mobility Management Function (AMF) exhibits the Namf service-based interface.

5G NF can offer different capabilities to distinct authorized consumers. According to ETSI TS 123 501 [i.2], an NF service is an offering of a specific capability, which is self-contained, reusable and uses management schemes independently of other NF services offered by the same NF (e.g. for scaling, healing, etc.). Clause 7.2 of ETSI TS 123 501 [i.2] specifies the list of NF services exposed by each NF through its service-based interfaces.

Furthermore, NFs and NF services (NF service consumers and NF service producers) can communicate directly, referred in ETSI TS 123 501 [i.2] as "Direct Communication", or indirectly via the Service Communication Proxy (SCP), referred as "Indirect Communication". Figure 5.3.1-2 illustrates the "Direct Communication" and "Indirect Communication" cases. The SCP does not expose services itself. The SCP can be deployed in a distributed manner. Whether an NF service consumer or NF service producer uses Direct Communication or Indirect Communication by using an SCP is based on the local configuration of the NF service consumer/producer.

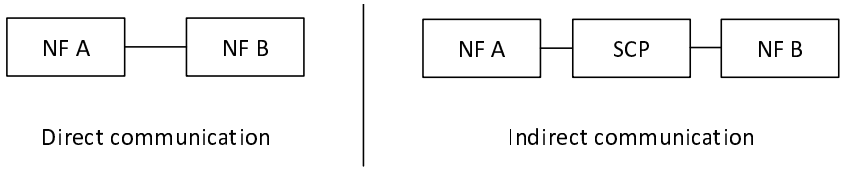


Figure 5.3.1-2: NF/NF service inter communication (from ETSI TS 123 501 [i.2])

Annex E of ETSI TS 123 501 [i.2] provides a high-level description of the different communication models that NF and NF services can use. Table 5.3.1-1 summarizes the different communication models.

Table 5.3.1-1: Communication models for NF/NF services interaction summary (from ETSI TS 123 501 [i.2])

Communication between consumer and producer	Service discovery and request routing	Communication model
Direct communication	No NRF or SCP; direct routing	A
	Discovery using NRF services; no SCP; direct routing	B
Indirect communication	Discovery using NRF services; selection for specific instance from the Set can be delegated to SCP. Routing via SCP	C
	Discovery and associated selection delegated to an SCP using discovery and selection parameters in service request; routing via SCP	D

ETSI TS 123 501 [i.2] describes the case in which an SCP deployment is based on a distributed model and implemented using (network wide) service mesh technology. In this model, SCP endpoints are co-located with 5GC functionality (e.g. an NF, an NF service, a subset of NF/NF service implemented as a microservice, or a superset of groups of NF, NF services or microservices). In this case, a deployment unit thus contains NF functionality and SCP functionality, as illustrated in figure 5.3.1-3. The SCP service agent is the SCP part co-located in the same deployment unit.

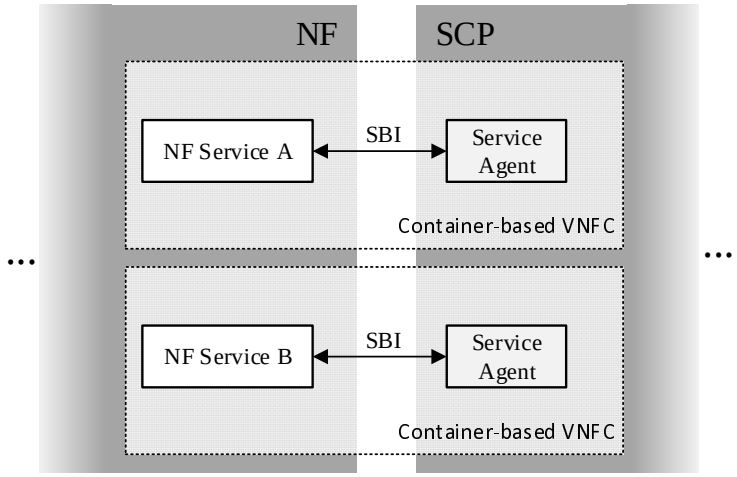


Figure 5.3.1-3: Detail of the NF-SCP boundary (from ETSI TS 123 501 [i.2])

ETSI TS 123 501 [i.2] also describes the case on which the SCP is deployed as independent deployment units.

For both direct communication and indirect communication to realize service-based interface, NRF resolves destination of target NF and authorization of NF service consumer as 5GC functionality specified in ETSI TS 123 501 [i.2].

5.3.2 Profiling of related NFV capabilities, features and specifications

5.3.2.1 General NFV concepts

The NFV information and data modelling provides the following capabilities to support different aspects of the "service-based interfaces, communication, and service mesh":

- Routing, resolve destination: Virtual Links (VL), virtual networks, VNF Forwarding Graph (VNFFG) and Network Forwarding Path (NFP).
- Self-contained, reusable and use of management schemes independently: VNF and VNFC, scaling aspects. For more information, see also the description about VNF componentization in clause 5.2.2.1.
- Exposure of connectivity points: VNF external Connection point (VnfExtCp).
- VM-based and container-based VNF.

Virtual Links and virtual networks

A VL is an abstraction representing the set of connection points along with the connectivity relationship between them and any associated target performance metrics (see definition in ETSI GR NFV 003 [i.1]). A VL can interconnect two or more entities. If connectivity is established at the NS level, VLs interconnect NS constituents such as VNF, PNF and nested NS. If connectivity is established at the VNF level, then VLs interconnect VNF constituents such as the VNFC. The VLs are realized by allocating virtual networks in the NFVI-PoPs and MSCSs across multi-sites (NFVI-PoPs).

A VL is managed by NFV-MANO based on a VL descriptor (VLD) and other runtime information. VLs can use different protocols at different layers (e.g. L2, L3, etc.) and specify concrete flow patterns for the connectivity (e.g. line, tree, mesh). A VLD indicates at least one element of the VL protocol stack, the top layer one. The VLD can also specify other deployment flavour attributes to consider further requirements related to QoS and service availability levels.

One important aspect regarding the VL concept is that it enables specifying the connectivity of sets of connection points, regardless of the intermediate connectivity elements that might be needed to ensure such a connectivity. In the absence of specified forwarding graphs (VNFFG), CPs that are participating into the connectivity to a certain VL are expected, by default, to be able to interconnect among each other according to the connectivity pattern. The NsVirtualLinkConnectivity information element specified in ETSI GS NFV-IFA 014 [i.9] is used to describe the connectivity information between the VNF or other constituents of the NS to the NS VL.

VNF Forwarding Graph and Network Forwarding Path

A VNFFG is a graph of logical links connecting NF for the purpose of describing specific traffic flows between the NF, and where at least one of the NF participating in the graph is a VNF (see definition in ETSI GR NFV 003 [i.1]). The VNFFG enables to define a specific topology of the NS, or a portion of it. It is created by referencing a pool of CP and service access points (SAP) and the constituents VNFs, PNFs and VLs that connect them. A VNFFG can also contain network forwarding paths (NFP), which associate traffic flows criteria to CPs and SAPs that are requested to be "visited" by the traffic flows matching the criteria. The sequence of CPs or groups of CPs to be traversed by the traffic flows is determined by the order position specified in the NFP descriptor (NFPD).

As a summary, with these constructs, traffic flow patterns can be determined, as well as the order in which to traverse the constituents in the NS.

VNF external Connection Point

A CP represents a point of connectivity of a constituent in the network, such as a VNF or a VNFC. A VNF's connection point that enables connectivity to external VLs of the VNF is a VNF External CP (in short, VnfExtCp). A CP can be connected to a VL and is managed by NFV-MANO. In the case a VnfExtCp is re-exposed as an SAP, it is not connected to a VL except in the case of a nested NS.

VM-based and container-based VNF

A VNF can have each of its VNFCs deployed as a VM or as a set of containers. A VNF can entirely be formed by container-based VNFCs, or VM-based VNFCs or a mix (i.e. some VNFCs based on container and some VNFCs based on VM). The unit of deployment, VNFC, is either mapped to:

- In the case of a VM-based VNFC, the VNFC is mapped 1:1 to a VM.
- In the case of a container-based VNFC, the VNFC is mapped 1:1 with an MCIO requesting compute/storage resources (refer to ETSI GS NFV-IFA 040 [i.31]). A Compute MCIO, described by the "Vdu" information element in the ETSI GS NFV-IFA 011 [i.12], can have one or more OS containers.

The VDU in the VNFD describes the deployment and resource requirements aspects of a VNFC. Based on the VNFC concept, the deployment of a VNF can be distributed across different compute hosts on the NFVI, across different resource zones, and even across different NFVI-PoPs (sites). In this regard, the VNF deployment can be distributed.

5.3.2.2 Specific profiling aspects and specification references

ETSI GR NFV-IFA 029 [i.16] documents use cases and concepts related to Platform as a Service (PaaS) capabilities. Specifically, use cases related to VNF Common and Dedicated Services are documented. These services can be provided to a consumer VNF, and can involve services such as messaging, databases, logging, etc. A VNF Common Service can be shared by several consumer VNF and a consumer VNF instance can invoke one or more VNF Common Service instances. A VNF Common Service only provides one type of common function. In the case of VNF Dedicated Service, an instance of it can only be consumed by a limited set of consumer VNF instances. In addition, as documented in the use cases of the referred document, the VNFD is expected to contain information about the dependencies or requirements the consumer VNF has on VNF Common or Dedicated Services. A possible way to realize these services is also implementing them based on OS containers.

5.3.3 Potential solutions

5.3.3.1 Solution #2A: VL abstracts 5GC control plane service mesh in direct communication (5GC communication model A)

The present solution addresses the baseline 5GC communication model A wherein neither NRF nor SCP is provided, and the communication among 5GC NF takes places directly and using standard routing solutions.

In this solution, the NF are configured with the appropriate "NF profiles" of the other peer NFs in the 5GC, and the communication then takes place directly. However, in this case, since the configuration to connect to other NF is based on either FQDN or IP addresses layer 3 network connectivity is expected to be available for the 5GC NF and NF services.

Considering this scenario, VLs can be used to abstract the connectivity for enabling the communication among the 5GC NF and NF services. NS VL can abstract the connectivity at various network layers, including L3. The "layerProtocol" of the "ConnectivityType" of the "NsVirtualLinkDesc" defined in ETSI GS NFV-IFA 014 [i.9] supports the definition of IPv4 and IPv6 as a requirement for the deployment of the NS VL. In addition, the "L3ProtocolData" information element allows the NS designer to specify requirements about the L3 protocol capabilities such as ranges of IP addresses allocation pools and the Classless Inter-Domain Routing (CIDR) of the network.

Figure 5.3.3.1-1 illustrates an example of this solution.

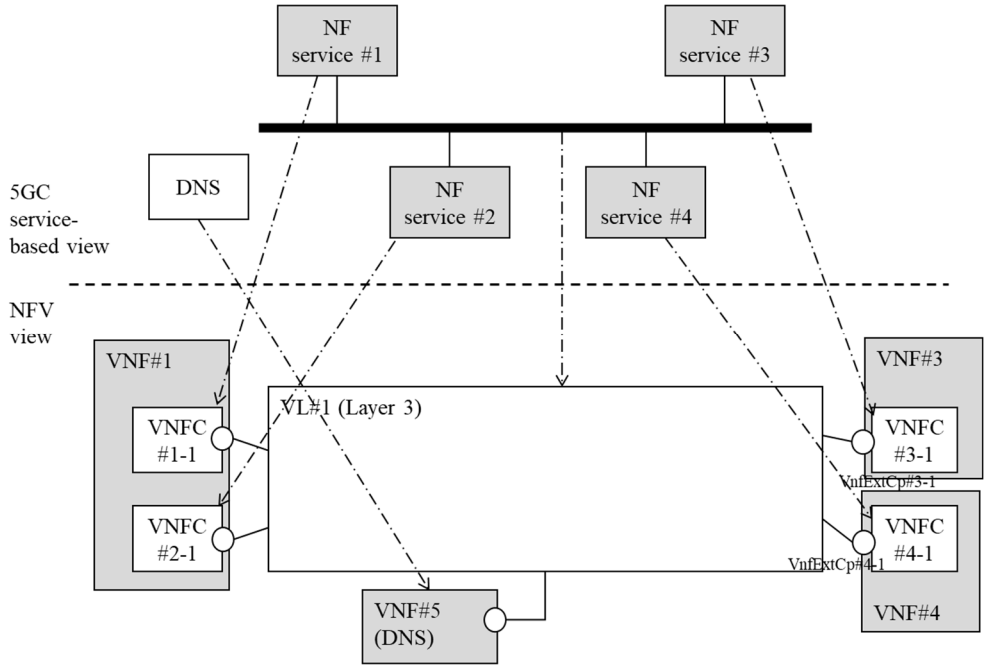


Figure 5.3.3.1-1: Example of Solution #2A: VL abstracts 5GC control plane service mesh in direct communication (5GC communication model A)

5.3.3.2 Solution #2B: VL abstracts 5GC control plane service mesh in direct communication (5GC communication model B)

5.3.3.2.1 Overview

In this set of solutions, the NS VL abstracts the 5GC control plane service mesh. Figure 5.3.3.2.1-1 illustrates the baseline for the sub-solutions in Solution #2B.

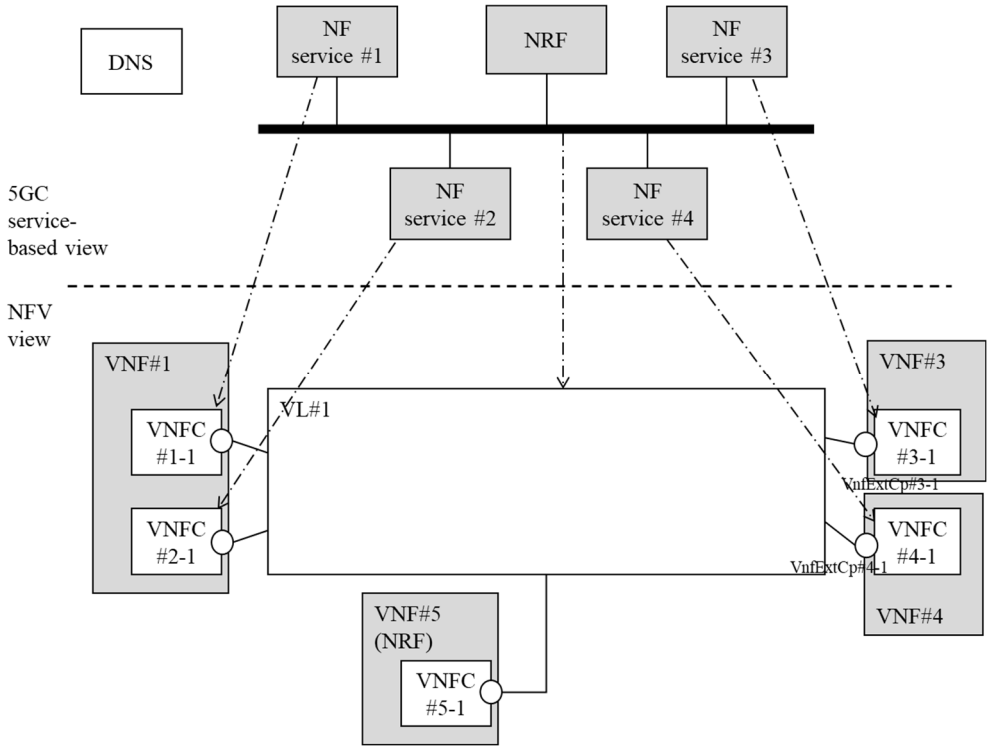


Figure 5.3.3.2.1-1: Baseline of Solution #2B

5.3.3.2.2 Solution #2B-A: No modification to NFV in direct communication

When VNF#1 as a consumer and VNF#2 as a producer communicates, VNF#1 discovers FQDN of VNF#2 from NRF (not depicted in figure 5.3.3.2.2-1) and resolves FQDN of VNF#2 by DNS as VNF. NFV-MANO provides VNF and VL capability to establish connectivity between VNF#1 and VNF#2 as described in figure 5.3.3.2.2-1.

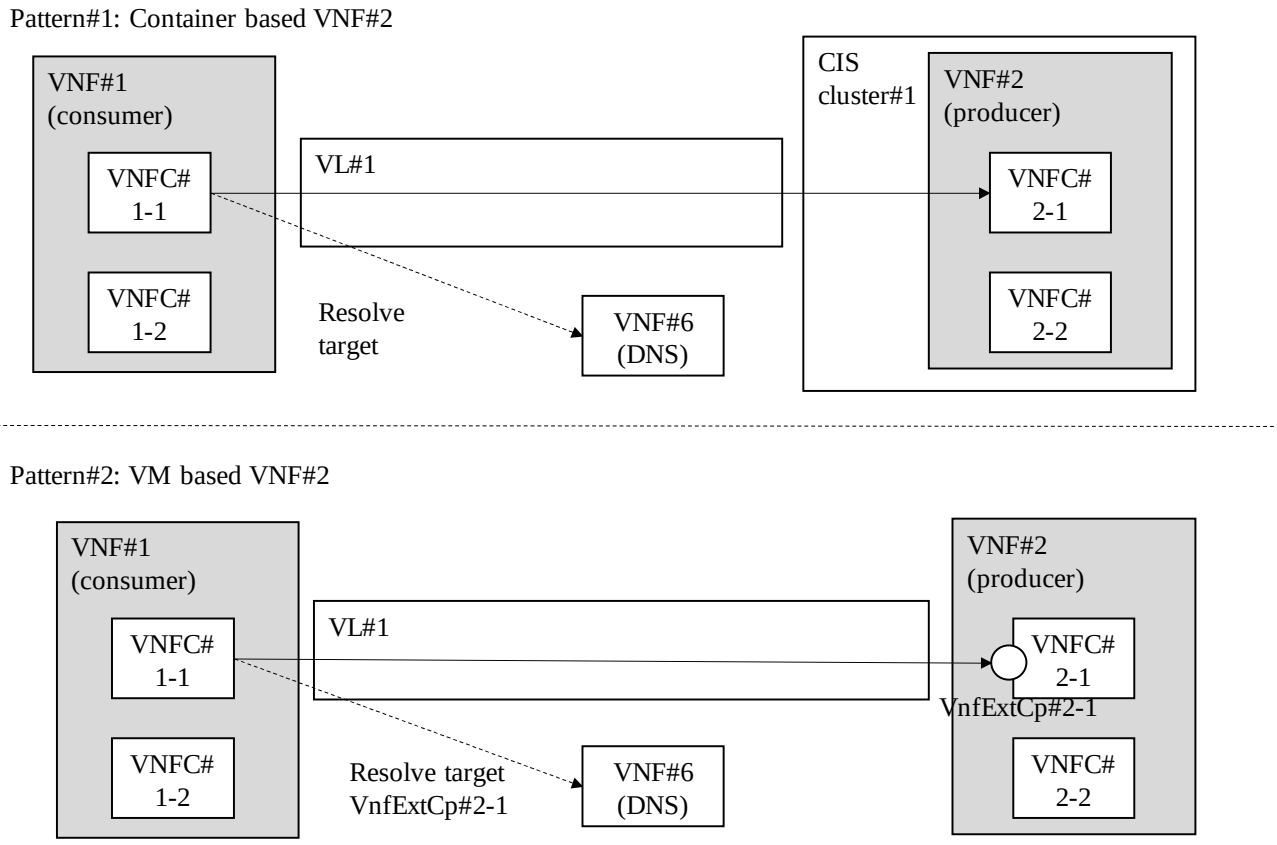
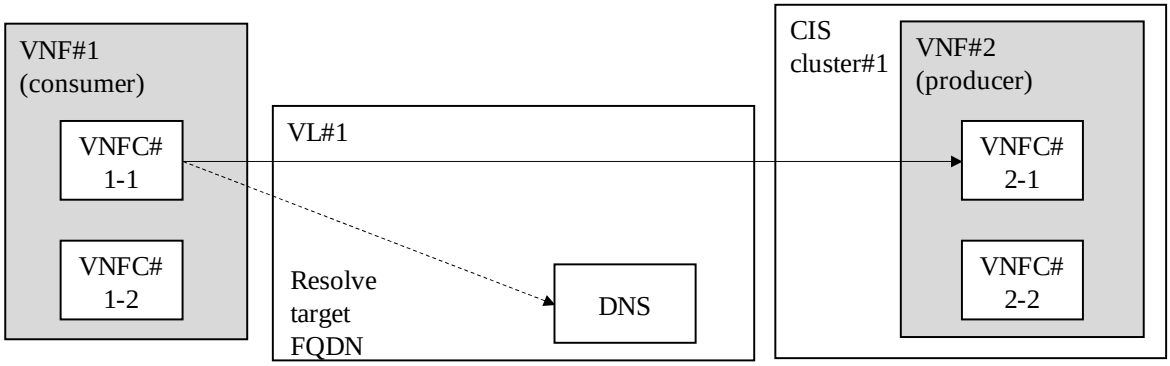


Figure 5.3.3.2.2-1: Example of Solution #2B-A: No modification to NFV in direct communication

5.3.3.2.3 Solution #2B-B: Enhance VL to support DNS resolving FQDN in direct communication

When VNF#1 as a consumer and VNF#2 as a producer communicates, VNF#1 discovers the FQDN of VNF#2 from the NRF (not depicted in figure 5.3.3.2.3-1). NFV-MANO provides extended VL capability that supports DNS resolving FQDN to establish connectivity between VNF#1 and VNF#2 as described in figure 5.3.3.2.3-1.

Pattern#1: Container based VNF#2



Pattern#2: VM based VNF#2

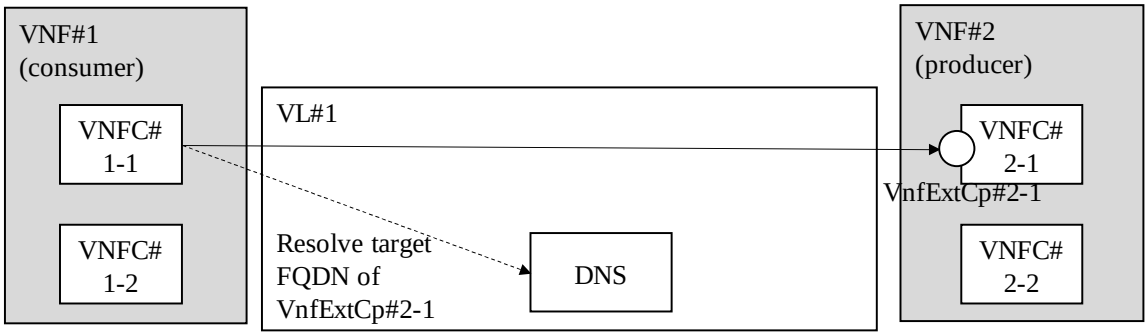


Figure 5.3.3.2.3-1: Example of Solution #2B-B: Enhance VL to support DNS resolving FQDN in direct communication

5.3.3.3 Solution #2C: NFV objects implement SCP for indirect communication

5.3.3.3.1 Overview

In this set of solutions, VNF and VNFCs implement NF and NF services. Indirect communication with SCP can be realized with various NFV capabilities. Figure 5.3.3.3.1-1 illustrates the baseline for the sub-solutions in Solution #2C.

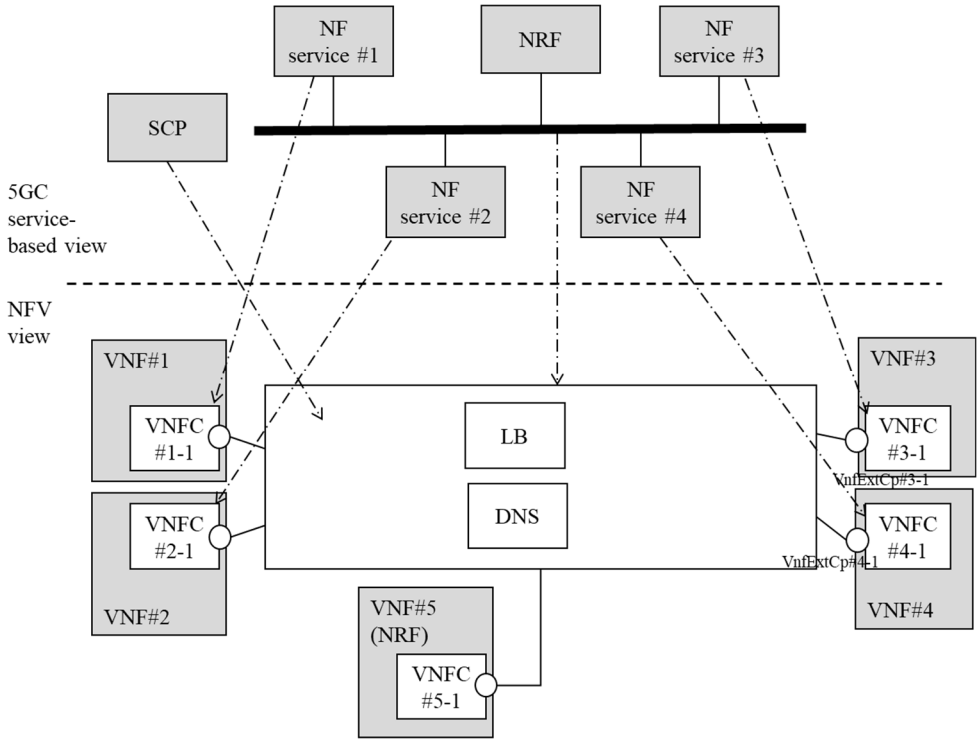


Figure 5.3.3.3.1-1: Baseline of Solution #2C

5.3.3.3.2 Solution #2C-A: Implement SCP by VNF

In this solution, VNF and VNFCs implement NF and NF services. In indirect communication case, an SCP enables VNFCs to communicate with each other in VM and container hybrid architecture. SCP can be deployed as a VNF. Multiple VNFCs can be accommodated with one SCP, thus DNS is usable for distinguishing NF services.

In this case, the sequence for sending packet to the destination endpoint (to NF service producer) can include:

- Resolve NF by NRF (not depicted in figure 5.3.3.3.2-1).
- Resolve SCP's IP address by DNS.
- Send packet to SCP.
- SCP checks DNS name to route packet to VNFC.
- SCP sends packets to VNFC.

Figure 5.3.3.3.2-1 illustrates an example of this solution.

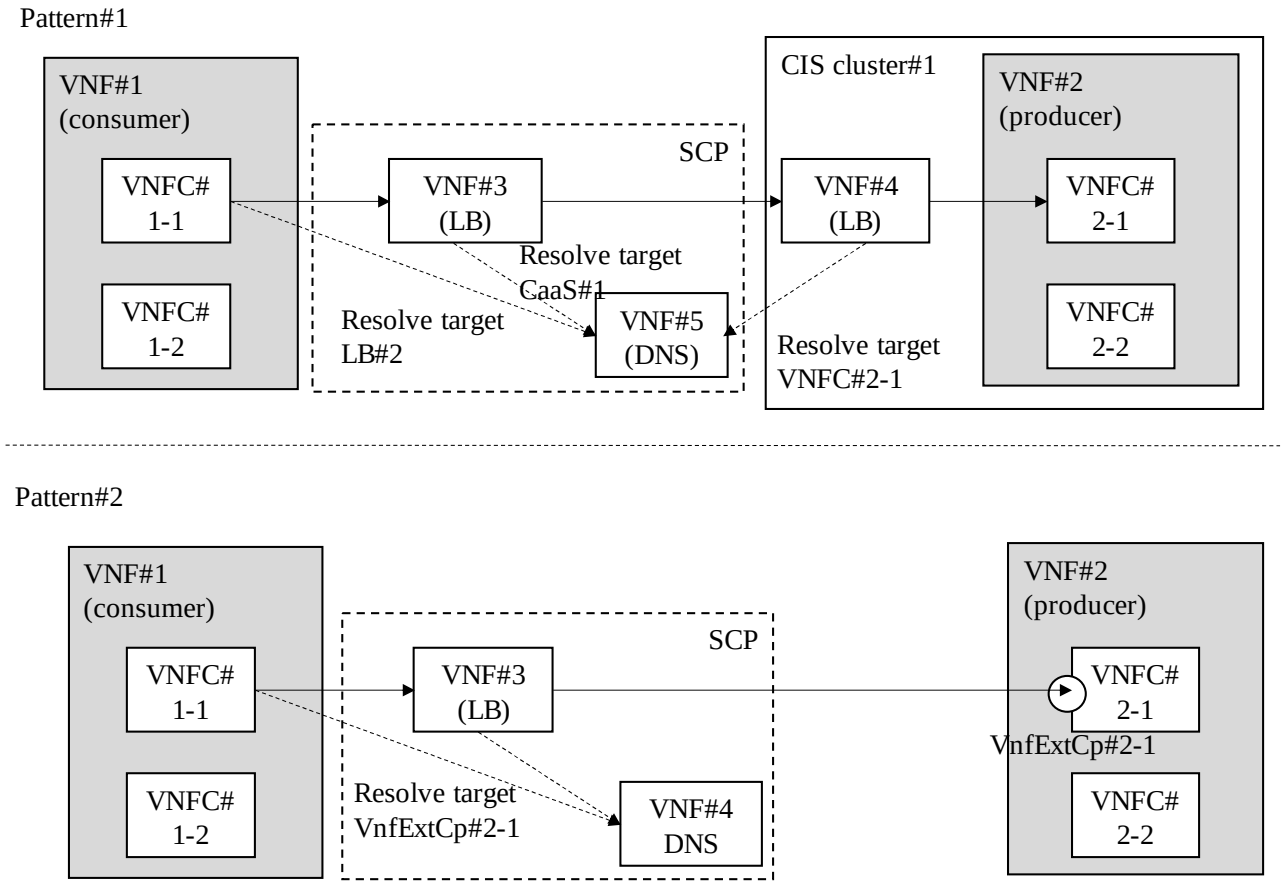


Figure 5.3.3.3.2-1: Example of Solution #2C-A: Implement SCP by VNF

5.3.3.3.3 Solution #2C-B: Implement SCP by VL

Based on #2C-A, this solution implements SCP's LB and DNS resolution functionality nested into VL as enhanced NS VL capability. Figure 5.3.3.3.3-1 illustrates an example of this solution, in which:

- A VL is extended to have LB and DNS functionality to connect consumer VNF#1 to producer VNF#2 as a part of SCP.
- NFV-MANO update configuration of VL#1 during the lifecycle management of VNF#1 and VNF#2.

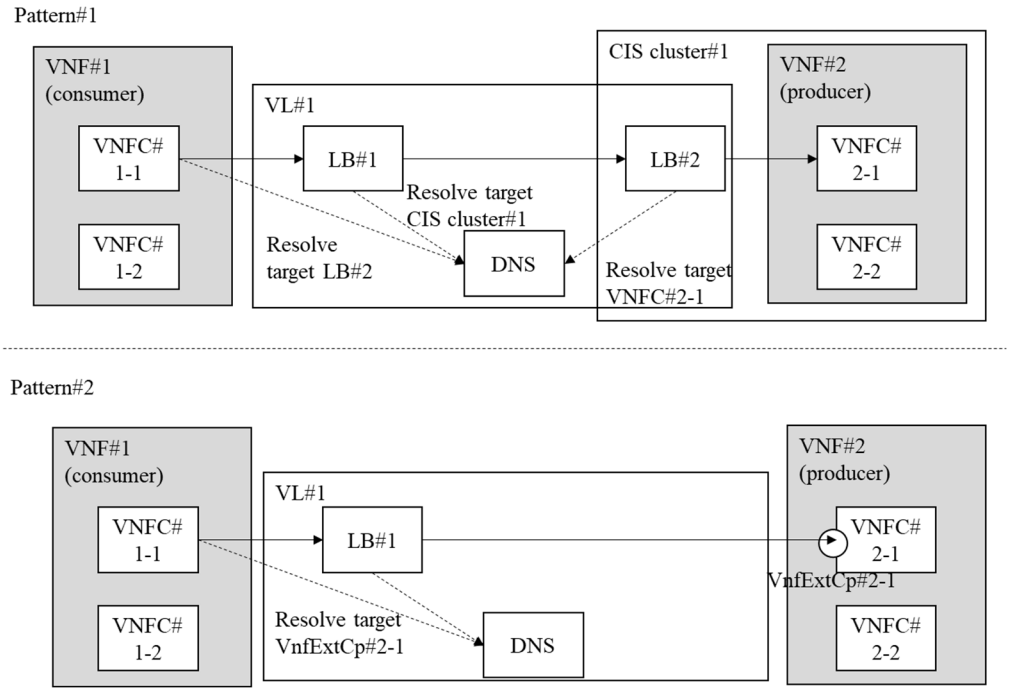


Figure 5.3.3.3.3-1: Example of Solution #2C-B: Implement SCP by VL

5.3.3.3.4 Solution #2C-C: Implement SCP by NFP

According to ETSI TS 123 501 [i.2], the SCP is responsible for forwarding and routing to destination NF/NF service. Also, according to the same referred 3GPP specification, load balancing, monitoring, overload control functionality provided by the SCP is left to the implementation from the 3GPP perspective.

Regarding the forwarding and routing, the NFP construct in NFV can be leveraged as the mechanism to steer packets on the network according to certain criteria. The NFP descriptor associates traffic flow criteria to a list of descriptors associated to the CP of the VNF (and PNF) and the SAP of the NS to be visited by the traffic flows matching the criteria.

This solution leverages the NFP construct to handle the "message forwarding and routing to destination NF/NF service" and the "load balancing" of messages. Figure 5.3.3.3.4-1 illustrates an example wherein two NFPs are defined to influence the routing and forwarding of messages on the network enabled by the VL#1. The NFP#1 is used to steer the control and data plan messages between VNF#1, VNF#2 and VNF#3 on corresponding external CPs. The NFP#2 is used to steer the traffic regarding access to the NRF and other network services/functions. The NFP configurations determine the configuration of underlying network resources to ensure that packets traverse a specified set of CPs, thereby performing the functionality to route the messages among 5GC NF/NF services.

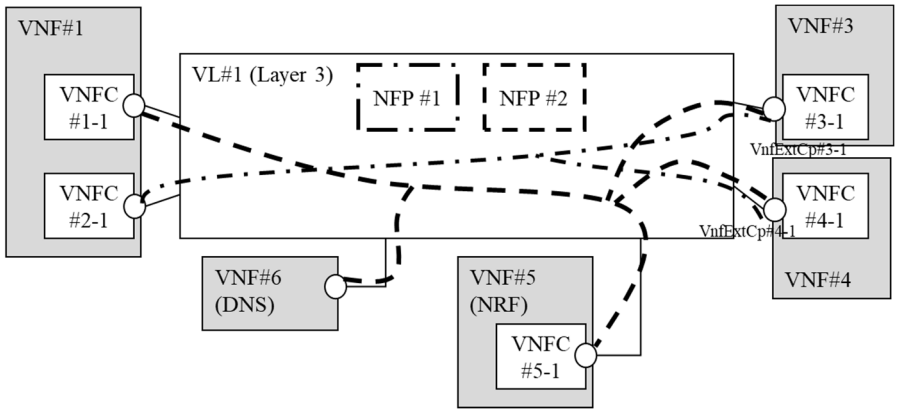


Figure 5.3.3.3.4-1: Example of Solution #2C-C: Implement SCP by NFP

5.3.3.4 Solution #2D: Container-based VNF with service mesh "sidecars"

This solution leverages the capabilities of the NFV framework to support the componentization of VNF and its distributed deployment. In addition, it also leverages the capability of container-based VNF wherein the VNFC can be composed of more than one OS container (see description in clause 5.3.2.1). In this scenario, one or more OS containers of the VNFC can be used to implement the specific 5GC NF service functionality, while other OS container can be used as dedicated service mesh agents, i.e. the "sidecar proxies", as part of the SCP deployment. Clause G.2.1 in Annex G of ETSI TS 123 501 [i.2] describes this same type of solution. Figure 5.3.3.4-1 illustrates this solution with a reference to the referred Annex of ETSI TS 123 501 [i.2].

For enabling the control plane functionality of the service mesh, i.e. deployment of the service mesh controller(s) and functions for the internal services registration and discovery (refer to figure G.2.1-1 in clause G.2.1 of ETSI TS 123 501 [i.2]), Solution #2C-A can be leveraged, i.e. deploy the control plane functionality as a VNF. The control plane functional of the service mesh can also be deployed as a VNFC when the service mesh scope is internal to a VNF, or it can also be deployed as a VNF Common Service.

In terms of enabling the data plane functionality of the service mesh, i.e. deployment of the service mesh agent and its attachment to the NF Services (as illustrated in figure 5.3.3.4-1) for the transfer and forward of packets, two options are considered:

- Option A: The VNF Package of the VNF to deploy includes and/or refers to the related OS container software images of the "sidecar proxy" implementing the service agent of the SCP. The VNFD also describes the relevant structure of the VDU and the expected deployment of the Compute MCIO including all the necessary OS containers, including the "sidecar proxy" ones.
- Option B: The VNF Package of the VNF to deploy includes and/or refers to the OS container software images for the Compute MCIO realizing the VNFC, but it does not refer to specific software images for the "sidecar proxy". In this case, the expected componentization to include such service agent is expressed via additional NFVI or VNF Common and Dedicated Services requirements, so that at the time that the Compute MCIO is to be deployed, the "sidecar proxy" is integrated by NFV-MANO.

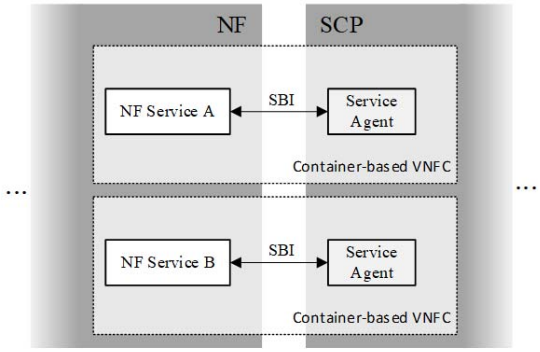


Figure G.2.1-3: Detail of the NF-SCP boundary

Figure 5.3.3.4-1: Example of Solution #2D: Implement SCP with container-based VNF with service mesh "sidecars" (figure extracted from ETSI TS 123 501 [i.2])

5.3.4 Gap analysis

The referred ETSI NFV specifications in the present characteristic profiling do not document:

Gap #2.1: For efficient integration of service-based interface in 5GC service mesh, NFV-MANO is expected to support NF integration of service mesh for VNF internal communication between VNFCs (VNF-level) and VNF external communication between VNFs (NS-level).

Gap #2.2: How to declare that a VNF can depend on specific VNF Common/Dedicated services, e.g. Vdu information element supports the specification of NFVI constraints and requested additional capabilities, but it does not support specifying PaaS capabilities related to communication (e.g. service mesh capabilities).

Gap #2.3: How NS VLs and VNF VLs can provide additional capabilities such as name resolution and load-balancing.

NOTE: Load balancing is supported via NFP, but with the absence of an NFP, there is no capability supported by the VL itself.

5.4 Characteristic #3: Network slicing

5.4.1 Introduction

From Release 15, 3GPP added support for "network slicing" as part of the design of the 5G system. ETSI TS 123 501 [i.2] defines a "Network Slice" as a logical network that provides specific network capabilities and network characteristics. A specific instance of a network slice is defined as the set of Network Function instances and the required resources (e.g. compute, storage and networking resources) which form a deployed network slice.

According to ETSI TS 123 501 [i.2], a network slice instance is defined within a Public Land Mobile Network (PLMN) and includes:

- the Core Network Control Plane and User Plane Network Functions, as described in clause 4.2,

and, in the serving PLMN, at least one of the following:

- the 5G radio access network (NG-RAN) described in ETSI TS 138 300 [i.4];
- the Non-3GPP InterWorking Function (N3IWF) or Trusted Non-3GPP Gateway Function (TNGF) functions to the non-3GPP Access Network described in clause 4.2.8.2 of ETSI TS 123 501 [i.2] or the Trusted WLAN Interworking Function (TWIF) to the trusted Wireless LAN (WLAN) in the case of support of Non-5G-Capable over WLAN (N5CW) devices described in clause 4.2.8.5 of ETSI TS 123 501 [i.2];
- the Wireline Access Gateway Function (W-AGF) to the Wireline Access Network described in clause 4.2.8.4 of ETSI TS 123 501 [i.2].

The diverse cases of composition of a network slice in the 5G system lead to extending the concepts of network slicing to consider the management of the network slices and the resource composition. From a management perspective, ETSI TS 128 530 [i.5] defines the concept of "network slice subnet", which represents a group of network functions (including their corresponding resources) that form part or complete constituents of a network slice. The grouping allows to conduct management of the subnets independently of the network slice. In addition, from a management perspective, a network slice instance is at least always mapped 1:1 to a network slice subnet instance. A network slice subnet instance can be decomposed recursively into other nested network slice subnet instances.

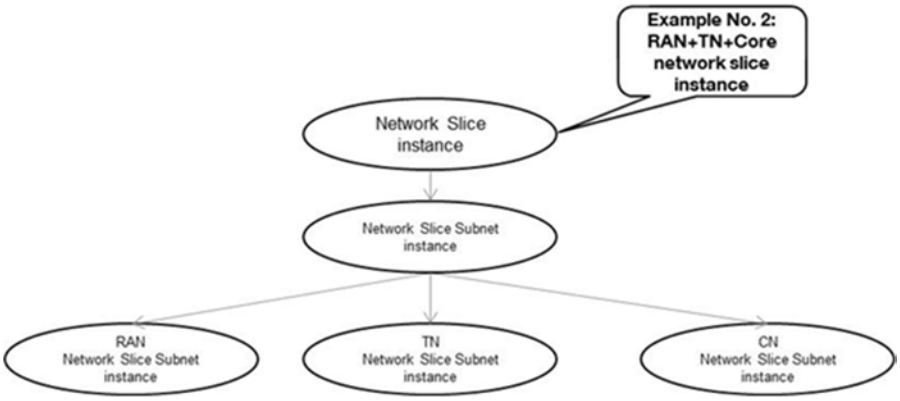


Figure 5.4.1-3: Example of RAN, Transport Network (TN) and Core Network (CN) network slice subnets exposed as a network slice (from ETSI TS 128 531 [i.39])

5.4.2 Profiling of related NFV capabilities, features and specifications

5.4.2.1 General NFV concepts

The NFV information and data modelling provides the following capabilities to support different aspects of the "network slicing" characteristic, including:

- Network Services (NS);
- VNF and PNF;
- Multi-Site Connectivity Services (MSCS);
- resource groups and multi-tenancy;
- NS management in multiple administrative domains; and
- affinity and anti-affinity constraints for NS and VNF constituents.

Network Services (NS)

An NS is a composition of NF(s) and/or NS(s). NS instances are managed by the NFVO based on the Network Service Descriptor (NSD) templates, runtime information created by the NFVO or retrieved from other NFV-MANO functional blocks via interfaces, and policy information.

VNF and PNF

While NFV-MANO fully manages the lifecycle of VNFs and the fault, configuration and performance of associated virtualised resources of the VNF, NFV-MANO is also able to manage the connectivity aspects for nesting Physical Network Functions (PNF) as constituents of an NS. PNF descriptors (PNFD) describe the PNF's external Connection Points (CP) and certain attributes such as geographical location.

Multi-site connectivity services (MSCS)

An MSCS is a connectivity service that abstracts the details of information regarding the connections between two or more NFVI-PoP (site) network endpoints. MSCS enable the support of connectivity for deployment cases where NS constituents (either VNF/PNF, nested NS, or both) are deployed in more than one site, as well as the connectivity for cases when the constituents of a VNF might also be distributed across sites.

Resource groups and multi-tenancy

NFV-MANO inherently supports multi-tenancy of NFV infrastructure resources as described in ETSI GS NFV-IFA 010 [i.6] at the functional requirement level. In particular the VIM supports grouping sets of virtualised resources into a "virtualised resource group" as specified in ETSI GS NFV-IFA 005 [i.30] and ETSI GS NFV-IFA 006 [i.19]. A virtualised resource group is assigned and used by a tenant, i.e. a consumer of virtualised resources from the NFVI, such as a VNFM, or a lower granular managed object, such as a VNF, or even external management systems acting as NFV-MANO consumers. Currently, "virtualised resource groups" are defined and managed by means out of scope of the referred specifications.

NS management in multiple administrative domains

From Release 3, NFV-MANO also supports the provisioning and management of NS across multiple administrative domains based on the interaction between NFVOs in different administrative domains supported over the Or-Or reference point. The administrative domains can correspond to different organizations, e.g. different network operators or different departments of the same network operator. In this scenario, the concept of composite NS and nested NS plays a key role as the form to compose NS across multiple administrative domains. ETSI GS NFV-IFA 030 [i.27] specifies the requirements and interfaces on the Or-Or reference point.

Affinity and anti-affinity constraints for NS and VNF constituents

Clause 5.5.2.2 in the present document describes about the aspects of affinity and anti-affinity constraints supported by the referred specifications. In addition, since v4.2.1 of the ETSI GS NFV-IFA 014 [i.9], affinity and anti-affinity constraints can also be applied to NS VL connectivity with scope of L2 network connectivity. With this capability, it can be determined that network resources realizing the NS VL are expected to support connecting the NS constituents into different or same L2 networks. This affinity/anti-affinity scope is in addition to the existing network link and node scope already supported since Release 3.

5.4.2.2 Specific profiling aspects and specification references

Clause 5.5 of ETSI GS NFV-IFA 010 [i.6] specifies the general requirements to support network slicing with NFV technologies and the NFV-MANO architectural framework. Clause 5.2 of the same referred specification also introduces the concepts of multi-tenancy and isolation between tenants, and the relationship by which resource groups, such as virtualised resource groups or service resource groups can be assigned to single or multiple tenants.

ETSI GS NFV-IFA 013 [i.10] specifies various enhancements to support network slicing use cases. For instance, the NS LCM interface on the Os-Ma-nfvo reference point was enhanced to support a new type of notification to notify about NS LCM capacity shortages which can occur when NS instances with higher-priority pre-empt other NS instances resources/LCM operations of lower priority. In addition, the NS LCM interface had also been enhanced to consider cases of pre-provisioning multi-site network connectivity across WAN(s) for fulfilling the NS and VNF VL connectivity. The attributes of an SAP of the NS, which represents the point of connectivity to/from the NS, support defining specific addressing for the SAP at various protocol layers.

Clause 5.3.2 of ETSI GR NFV-IFA 024 [i.7] describes the touchpoints between the 3GPP's network slicing management model and the ETSI NFV information model. In such a model, a network slice subnet is mapped N to 0..1 to an NS. Figure 5.4.2.2-1 illustrates such an information model touchpoint.

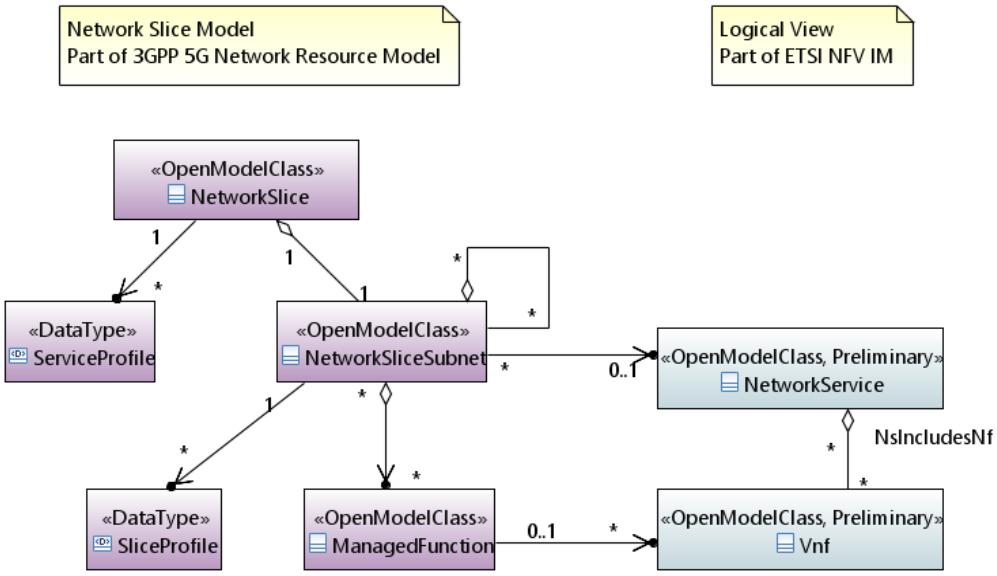


Figure 5.4.2.2-1: Touchpoints between NFV IM and Network Slicing Model (from ETSI GR NFV-IFA 024 [i.7])

5.4.3 Potential solutions

5.4.3.1 Solution #3A: Multiple NS as deployment unit for one network slice with NFV provided connectivity

In this solution, multiple NSs act as deployment units for one network slice. In the example illustrated in figure 5.4.3.1-1, the network slice is composed by three network slice subnets nested in another network slice subnet. Each of the network slice subnets is associated to a specific NS instance. The network slice subnet that nests the sub network slice subnets is also associated to an NS instance.

The network connectivity between the different network slice subnets is supported by the VLs (NS VL#4 and NS VL#5) interconnecting the set of nested NS through the exposed Service Access Points (SAP) of re-exposed VNF external connection points of VNF#1.1, VNF#2.1, VNF#2.2 and VNF#3.1.

Isolation of resources assigned to different network slice subnets can be achieved by declaring, in the NSD corresponding to NS#4, affinity/anti-affinity requirements between the nested NS instances created using different NS profiles. In addition, within the nested NS instances (NS#1, NS#2 and NS#3), the corresponding NSD can express affinity/anti-affinity requirements in between the constituent VNF, PNF and VL. If specific requirements of isolation at the network connectivity level are expected to be met among the constituents of the NS #1, NS#2, NS#3 and NS#4, this can be indicated via the respective NSD affinity/anti-affinity of NS VL connectivity by using the applicable "L2-network" and "network-link-and-node" scopes.

In addition to the affinity/anti-affinity requirements declared in the NSD, the NS lifecycle management interface exposed by the NFVO of NFV-MANO allows the consumer to signal as an input to the operations specific location constraints for the nested NS and VNF to be instantiated as part of the NS instantiation. An example is a constrain to instantiate a nested NS in a specific "geographical" location, such as the location of a specific NFVI-PoP.

This solution is also compatible on distributing the NS on multiple administrative domains. For instance, NS#1 could be mapped to the RAN part and be managed by the radio department of the network operator using a dedicated NFVO, while the other NS#2, NS#3 and NS#4 could be mapped to other parts of the network such as the CN or the data networks and be managed by other departments using another NFVO.

Figure 5.4.3.1-1 provides an example illustrating the concept of this solution.

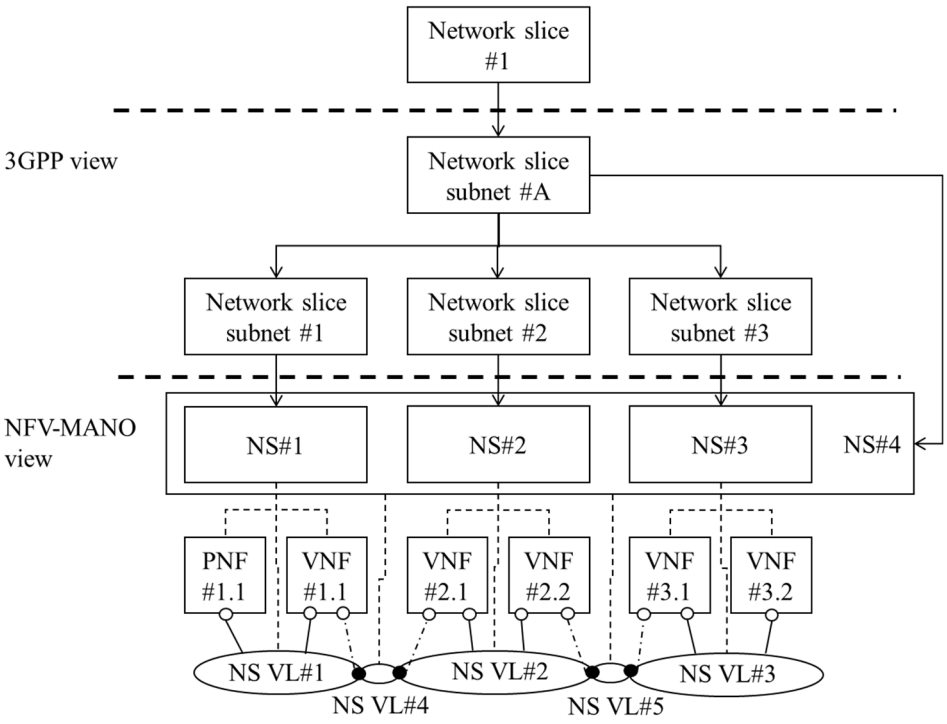


Figure 5.4.3.1-1: Example of multiple NSs to realize a network slice

5.4.3.2 Solution #3B: Multiple NS as deployment unit for one network slice without NFV provided connectivity for inter network slice subnet

In this solution, multiple NSs act as deployment units for one network slice. In the example illustrated in figure 5.4.3.2-1, the network slice is composed by three network slice subnets. Each of the network slice subnets is associated to a specific NS instance.

In this solution, the network connectivity between the different network slice subnets is assumed to be pre-provisioned and outside of NFV-MANO's responsibility.

NOTE: A mix of connectivity, i.e. pre-provisioned outside NFV-MANO and connectivity provisioned by NFV-MANO as described in Solution #3A in clause 5.4.3.1 is also possible. Therefore, the present solution and that other referred solution are introduced as the baseline cases on top of which more complex and mixed solutions can be built.

In this solution, isolation of resources assigned to different network slice subnets cannot be achieved in a declarative mode, i.e. by expressing in an NSD the affinity/anti-affinity requirements of corresponding 1:1 NS instances to network slice subnets. The reason is that there is no composite NS and associated NSD in which such requirement can be declared. Nonetheless, by using the NS lifecycle management interface exposed by the NFVO of NFV-MANO, the consumer (e.g. network operator's OSS/BSS) can signal as an input to operations specific location constraints for each of the NS and VNF to be instantiated as part of each individual NS instantiation for NS#1, NS#2 and NS#3. An example is a constrain to instantiate an NS in a specific "geographical" location, such as the location of a specific NFVI-PoP. If specific requirements of isolation at the network connectivity level are expected to be met among the constituents of the NS #1, NS#2, NS#3, this can be indicated via the respective NSD affinity/anti-affinity of NS VL connectivity by using the applicable "L2-network" and "network-link-and-node" scopes.

Furthermore, NFV-MANO supports the handling of resource tenancy by using the concept of "virtualised resource groups" as described in clause 5.4.2.1. This can be used to logically group and isolate virtualised resources on the NFVI. For instance, the resources used by each one of the VNF in this solution, and therefore by their respective NSs, can be assigned to different virtualised resource groups.

Figure 5.4.3.2-1 provides an example illustrating the concept of this solution.

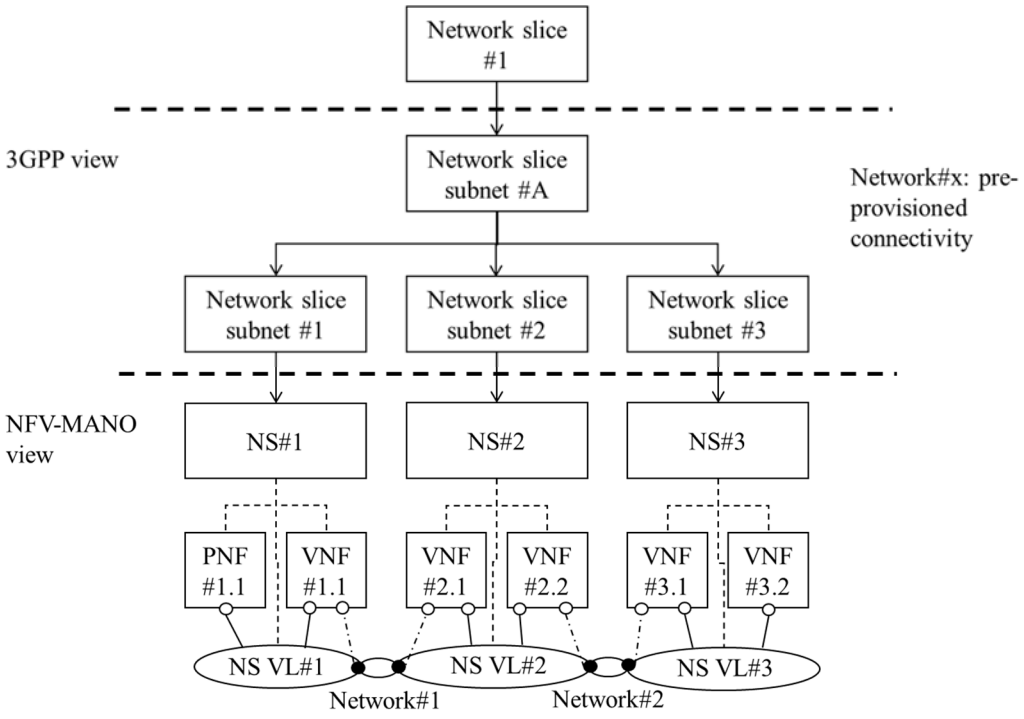


Figure 5.4.3.2-1: Example of multiple NSs to realize a network slice without NFV provided connectivity for inter network slice subnet

5.4.3.3 Solution #3C: A single NS as deployment unit for one network slice

In this solution, an NS acts as a deployment unit for one or more network slice subnets which deliver a network slice. As presented in clause 5.4.2, an NS instance can be associated to one or more network slice subnets.

The network connectivity between the different network slice subnets is supported by the actual connectivity of appropriate VNF external CPs to the respective NS VLs (NS VL#1, NS VL#2, and NS VL#3).

Isolation of resources assigned to different network slice subnets can be achieved by declaring, in the NSD corresponding to NS#1, affinity/anti-affinity requirements between the VNF instances created using different VNF profiles. However, since there is no specific parts in the NS#1 that map to specific network slice subnets (i.e. there is no indication in the NSD about specific groups of constituents in the NS), only about the VNF/PNF that compose them, such assignment of affinity/anti-affinity requirements is expected to be realized at the VNF/PNF level. If specific requirements of isolation at the network connectivity level are expected to be met among the constituents of the NS#1, this can be indicated via the respective NSD affinity/anti-affinity of NS VL connectivity by using the applicable "L2-network" and "network-link-and-node" scopes.

In addition to the affinity/anti-affinity requirements declared in the NSD, the NS lifecycle management interface exposed by the NFVO of NFV-MANO allows the consumer to signal as input to the operations specific location constraints for the VNF to be instantiated as part of the NS instantiation. An example is a constrain to instantiate a VNF in a specific "geographical" location, such as the location of a specific NFVI-PoP.

NOTE: By comparing Solutions #3A, #3B and #3C, it can be concluded that depending on the solution, the NS designer is expected to consider that in order to declare isolation requirements via affinity/anti-affinity constraints, the scope and members of the affinity/anti-affinity groups will be different. In case #3A, affinity/anti-affinity constraints can be declared among NSs that map 1:1 to network slice subnets, while in case #3C, the declaration of affinity/anti-affinity constraints can be declared only among constituent VNF and PNF of the only NS that maps 1:N to network slice subnets.

Figure 5.4.3.3-1 provides an example illustrating the concept of this solution.

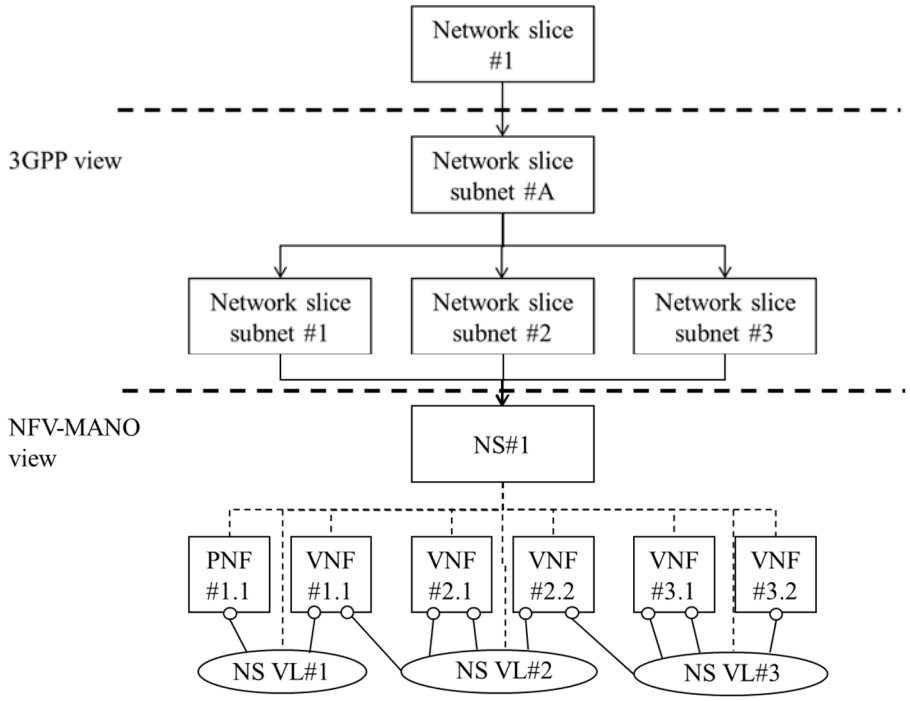


Figure 5.4.3.3-1: Example of an NS instance realizing a whole network slice

5.4.3.4 Solution #3D: Management of network slice transport network connectivity with multi-site connectivity services

In this solution, a network slice NS is composed of two or more network slice subnets. The network slice subnets are composed by VNF and PNF that are expected to be deployed on different geographical sites. Between these two sites, transport network resources are necessary for interconnecting the NFs. Figure 5.4.3.4-1 illustrates an example with two network slice subsnets, each composed of two network functions.

When the resource fulfilment is provided by NFV, the two network slice subnets are mapped to a single NS instance. The NS instance includes a VL which is realized by virtual networks and MSCS across sites (NFVI-PoPs). The transport network used to interconnect the network functions placed on different sites is provided by the MSCS. The MSCS is managed directly by the NFV-MANO with the WIM.

Similarly as with other solutions, if specific requirements of isolation at the network connectivity level are expected to be met among the constituents of the NS #1, this can be indicated via the respective NSD affinity/anti-affinity of NS VL connectivity by using the applicable "L2-network" and "network-link-and-node" scopes.

In this solution, NFV-MANO is able to provide all the necessary resource provisioning capabilities to instantiate a network slice possibly composed of various VNF and PNF spread across different sites.

Figure 5.4.3.4-1 provides an example illustrating the concept of this solution.

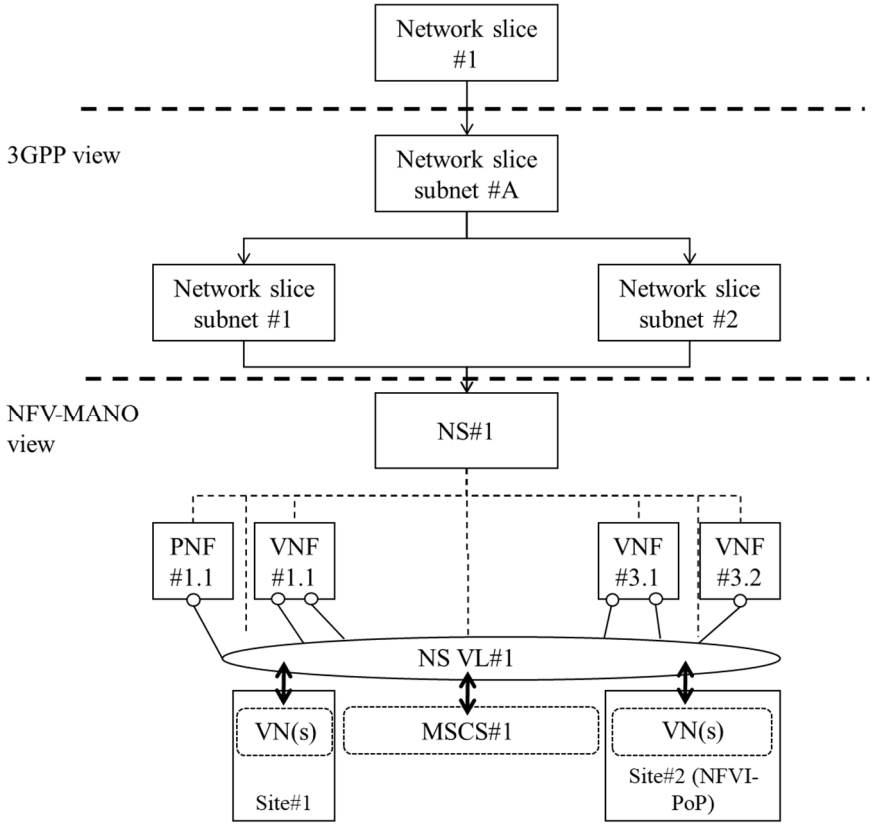


Figure 5.4.3.4-1: Example of an NS instance with transport network managed with MSCS

5.4.4 Gap analysis

The referred ETSI NFV specifications in the present characteristic profiling do not document:

Gap #3.1: Support for providing via the NS LCM interface information about expected values of L2 networks where the constituents of the NS with service access exposure (i.e. NS constituents with CPs which are mapped to SAP) are expected to be connected, in particular if some pre-provisioning of networking has been performed by the OSS/BSS and the CPs of the NS constituents are not in trunk mode.

5.5 Characteristic #4: Distribution of services across the network

5.5.1 Introduction

From Release 15, 3GPP designed the 5G system with the principle of separating User Plane (UP) functions from Control Plane (CP) functions to allow independent scalability, evolution and flexible deployment with the possibility to deploy functions either at a centralized location or distributed (remote) locations (refer to ETSI TS 123 501 [i.2]).

In the particular case of the 5GC, ETSI TS 123 501 [i.2] describes the different scenarios for supporting virtualised deployments, including, but not limited to, the following:

- An NF instance can be deployed as a distributed, redundant, stateless, and scalable NF instance that provides the services from several locations, or enables several execution instances at each location, e.g. a data center.
- An NF instance can also be deployed such that several NF instances are present within an NF Set that is distributed, redundant, stateless and scalable as a set of NS instances.

Within the 5GC, although not referred as NF instances:

- the SEPP can also be deployed in a distributed, redundant, stateless and scalable manner; and
- the SCP can also be deployed in a distributed, redundant and scalable manner.

NF instances of the same type can be grouped into an "NF Set" supporting the same services and same network slices, such as AMF instances in the same AMF Set, can be geographically distributed, but have access to the same context data. The concept is also applicable to NF Services. In this scenario, the network reliability can be increased thanks either to the NFs and NF Services sharing the same context data or the NF/NF Service Context Transfer procedures being applied as specified by ETSI TS 123 502 [i.8].

The NF Set works in both communication modes, i.e. Direct Communication and Indirect Communication (see also clause 5.3 of the present document). In the Direct Communication mode, the NF Service consumer is involved in the reliability related procedures. In Indirect Communication mode, the SCP is involved in such procedures.

Distribution of services across the network has implication in features such as the selection of NF and NF Services. For instance, according to ETSI TS 123 501 [i.2] the selection or reselection of the User Plane Function (UPF) is performed by the Session Management Function (SMF) by considering UPF deployment scenarios such as centrally located UPF and distributed UPF located close to or at the access network site among other information such as UPF supported capabilities.

In the 5G CN, the NRF maintains information (profiles) about the available NF instances and SCP instances. The profile contains information about locality of the NF or SCP instance. The location information is operator specific, but as an example, it can refer to geographical location or data center.

The 5G System also considers specific support for edge computing. Edge computing enables network operators and third-party services to be hosted close to the UE's point of attachment to achieve reduced end-to-end latency and efficient network load steering on the transport network. Some of the enablers of 5G CN that support edge computing are (not exhaustive list): user plane (re)selection, local routing and traffic steering, UPF (re)selection influenced by an Application Function (AF), and support of local area data network. The support of edge computing is relevant to the distribution of services across the network, since the aim is to steer UE's traffic into distributed and local networks closer to the access network points of the UE.

5.5.2 Profiling of related NFV capabilities, features and specifications

5.5.2.1 General NFV concepts

The NFV information and data modelling provides the following capabilities to support different aspects of the "distribution of services across the network " characteristic, including:

- location constraints for NS and VNF placement;

- affinity/anti-affinity constraints for NS constituents and VNF and VNF constituents (e.g. VNFC);
- PNF's location information in the PNFD;
- NS and VNF profiles; and
- Multi-Site Connectivity Services (MSCS).

Location information associated to NS and VNF placement and affinity/anti-affinity constraints

As part of the NFV-MANO's resource orchestration, requirements and/or constraints about the location for the NS constituents such as VNF are considered by NFV-MANO during the resource orchestration and assignment of virtualised resources to the NS constituents. In addition, affinity/anti-affinity constraints and relationships between the constituents of the NS and VNF are considered by the NFV-MANO to determine the assignment of virtualised resources.

PNF location information

PNF descriptors (PNFD) describe the PNF's external Connection Points (CP) and certain attributes such as geographical location.

NS and VNF profiles

A VNF profile specifies the characteristics for instantiating VNFs of a particular NS DF according to a specific VNFD and VNF DF. The characteristics include specific requirements for affinity/anti-affinity, number of instances that can be instantiated, connectivity information to the NS and service availability levels.

Similarly, an NS profile specifies the characteristics for instantiating nested NS of a particular NS DF, with similar characteristics as those defined in VNF profiles.

Multi-Site Connectivity Services (MSCS)

Refer to the description in clause 5.4.2.1.

5.5.2.2 Specific profiling aspects and specification references

Location information about a PNF can be provided in the PNFD as specified in clause 6.6.2 in ETSI GS NFV-IFA 014 [i.9]. The attribute "geographicalLocationInfo" of the "Pnfd" information element is used for such purpose. Protocol and data model solutions consider different forms to express location information such as country codes, civic address or geographic coordinates (e.g. altitude, longitude, latitude).

The capability to provide location constraints requirements is supported by the NS LCM interface produced by the NFVO towards the OSS/BSS. VNF location constraints can be expressed via the "VnfLocationConstraint" information element, and the location constraints of nested NS can be expressed via the "NestedNsLocationConstraint" information element specified in clauses 8.3.4.4 and 8.3.4.47 of ETSI GS NFV-IFA 013 [i.10], respectively.

In addition, the NSD information model specified in ETSI GS NFV-IFA 014 [i.9] enables the description of affinity/anti-affinity relationships applicable between the VNF instances, Virtual Link instances and nested NS instances of an NS:

- The "AffinityOrAntiAffinityGroup" describes the affinity/anti-affinity relationship applicable between instances of VNF, VL or nested NS created from different VNF, VL or NS profiles.
- The "LocalAffinityOrAntiAffinityRule" enables to express the affinity/anti-affinity constraints in between instances of VNF, VL or nested NS created from the same VNF, VL or NS profile.

Protocol and data model specifications, such as ETSI GS NFV-SOL 001 [i.11] define the concrete possible values of the scope that can be used for the affinity/anti-affinity relationship in the NSD and VNFD, including: "NFVI-PoP", "Zone", "ZoneGroup", "NFVI-node", "network-link-and-node". ETSI NFV Release 4 extends the list of scopes by adding "CIS-node" and "container-namespace" (more information is available in Annex B of ETSI GS NFV-IFA 011 [i.12]) and "L2-network" (more information is available in Annex B of ETSI GS NFV-IFA 014 [i.9]).

Within the NFV-MANO framework, VNF LCM procedures include interactions between the NFVO, VNFM and VIM for determining the actual instantiation of virtualised resources that realize the VNF and other NS constituents. The "PlacementConstraint" information element specified in clause 8.3.6 of ETSI GS NFV-IFA 007 [i.13] enables the VNFM to signal the NFVO during the granting of VNF LCM operations up-to-date placement constraints that not only indicate the actual relationships of virtualised resources to be newly instantiated for a new VNF, but also the relationship considering existing instantiated virtualised resources.

5.5.3 Potential solutions

5.5.3.1 Solution #4A: NS deployment for distributed 5GS with NFV-provided connectivity

Solution #4A focuses on the aspects of network connectivity for distributed 5GS. In this solution, an NS is used to deploy the NFs for a 5G CN. Network connectivity between the NF is expected to be fulfilled via several networks. The NS VLDs are used to define the requirements for network connectivity.

The 5G CN deployment considers distributing UPFs at several locations close to the RAN access points to enable routing the traffic to local data networks providing edge computing services. The deployment of UPFs is expected to leverage the NFVI-PoPs deployed at the edge and closer to the cell sites. Remaining NFs of the 5G CN are considered to be deployed centrally at a central site/office.

The NS LCM capabilities also enable the network operator not only to consider static deployment of the 5G CN, but also dynamic updates that can arise during the lifetime of the 5G CN such as adding or removing specific NF to/from the network to address load or new location requirements.

Figure 5.5.3.1-1 provides an example illustrating the NS deployment described above. Two views are illustrated: first, the NFV logical view which contains the NS composition, constituents and NS VL used to represent the connectivity among the NS constituents. Second, the deployment view which shows the deployment of specific VNF to respective NFVI-PoPs.

The key aspect to highlight from figure 5.5.3.1-1 is the capability of NFV-MANO to orchestrate and manage the connectivity among the NFs of the 5GS by setting up virtualised networks within the NFVI-PoPs as well as stitching the intra-DC/site connectivity to other connectivity enabled across transport network domains such as fronthaul, backhaul and WAN via the multi-site connectivity services managed by the WIM. This capability offers a holistic approach to the Service Provider to consider all aspects for the deployment including the location of NFs together with the fulfilment of connectivity for enabling end-to-end distributed 5G services.

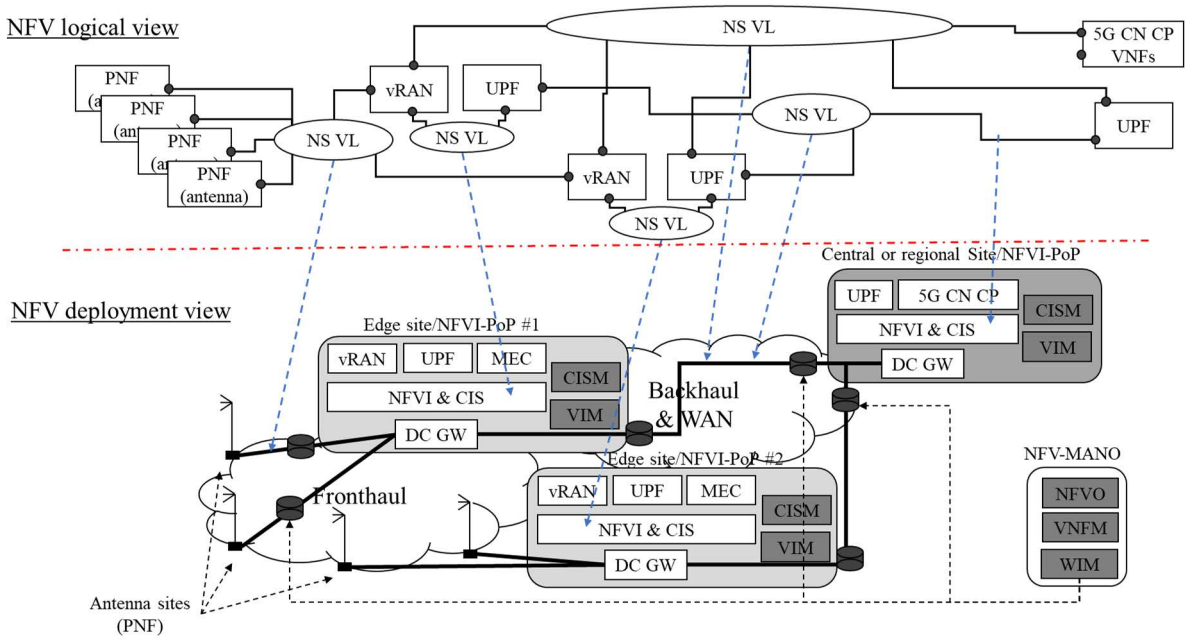


Figure 5.5.3.1-1: Example of distributed 5G CN with NFV-provided connectivity

5.5.3.2 Solution #4B: NS LCM with location and affinity/anti-affinity constraints

Solution #4B focuses on the aspects of fulfilling the placement for the constituents of a distributed 5GS.

Taking the example depicted in figure 5.5.3.1-1, NFV-MANO can determine the placement of NF across the network and at the different NFVI-PoPs as an explicit request from the OSS/BSS, as a consumer of the NS LCM interface produced by the NFVO. The specified affinity/anti-affinity constraints in the NSD are also used to determine the placement of the constituents based on the expressed placement relationships. As described in clause 5.5.2.2, the interfaces and descriptors enable the network designer to express all this.

As an example of the present solution, the deployment view could be realized by using the following constraints and placement requirements:

- vRAN in NFVI-PoP #1: OSS/BSS can provide specific location constraints to deploy the vRAN at the NFVI-PoP#1 by indicating geographic/civic information that is associated to the NFVI-PoP #1.
- vRAN in NFVI-PoP #2: same as above but indicating geographical/civic information that is associated to the NFVI-PoP #2.
- UPF in NFVI-PoP #1: NSD defines an "affinity group" at the NFVI-PoP scope level between the VnfProfile for such UPF and the VnfProfile(s) for the vRAN in NFVI-PoP #1.
- UPF in NFVI-PoP #2: same as above but establishing the relationship between the VnfProfile of the UPF and the VnfProfiles(s) for the vRAN in NFVI-PoP #2.
- 5G CN CP in central/regional NFVI-PoP: OSS/BSS can provide specific location constraints to deploy the 5G CN CP VNFs at the central/regional NFVI-PoP by indicating geographic/civic information that is associated to such NFVI-PoP.
- UPF in central/regional NFVI-PoP: NSD defines an "affinity group" at the NFVI-PoP scope level between the VnfProfile for such a UPF and the VnfProfile(s) for the VNFs composing the 5G CN CP.

5.5.3.3 Solution #4C: VnfProfiles for setting up NF/NF Service Sets

Solution #4C focuses on the aspects of NF/NF Service Sets as a key element for maintaining higher service availability and of distributed 5GS.

As introduced in clause 5.5.1, NF/NF Service Sets of a same type of NF/NF Service can be centralized at a location or be distributed geographically.

NOTE: This solution and the applicability to NF Service Sets leverages Solution #1B described in clause 5.2.3.2.

The concept of VNF profile supports the resource management and orchestration for NF/NF Service Sets with the following characteristics:

- VNF profiles support declaring a minimum and maximum number of VNF instances that can be created with a given VNF profile.
- VNF profiles support declaring affinity/anti-affinity rules for the VNF instances that are created using such a profile. This enables the capability to either affine or anti-affine NF instances in an NF Set according to a given scope, such as NFVI-PoP.
- All VNF instances created from a VNF profile are connected to the same NS VL, thus sharing same connectivity context and reachability.

As described in clause 5.7, different combinations of allocating stateful NF and NF Services are possible such as using virtual storage as part of a VNF, dedicating specific stateful VNF or reusing common functionality by the platform as a storage component.

5.5.3.4 Solution #4D: Distributed deployment of an NF

Solution #4D focuses on the aspect of distributed deployment of an NF to support distributed 5GS with redundant and scalable NF instance service from several locations. As described in clause 5.5.1, ETSI TS 123 501 [i.2] describes the possibility of deploying an NF instance in a distributed manner that can provide services from several locations.

For realizing this case, the solution leverages the following aspects:

- Support of connectivity across locations: the MSCS enables the internal connectivity of a VNF across the transport network or WAN. NFVO is responsible for managing the internal VL of the VNF composing network resources on the WAN and in the NFVI-PoPs. The internal VL is exposed to the VNFM and VNF as an "externally-managed VL" (refer to clause 8.5.10 of ETSI GS NFV-IFA 007 [i.13]).

- Support for execution units of VNF to be distributed: the use of affinity/anti-affinity enables the designer to request the deployment of VNFC, either derived from the same VDU or from different VDU, across different domains and locations by using the "NFVI-PoP" scope. For instance, if NF is expected to offer its services from different locations, VNFC associated to the delivery of the service can be deployed with explicit "NFVI-PoP anti-affinity constraints".

Figure 5.5.3.4-1 illustrates an example wherein the SMF is distributed across two NFVI-PoPs. The SMF's NF Service set "S1" is deployed on the edge site, while the NF Service set "S2" is deployed on the central or regional site. The first service set is delivered with a set of VNFC named VNFC#1, and the second set with VNFC#2.

NOTE: Currently, from an OSS/BSS perspective, it is not possible to explicitly indicate what NFVI-PoPs or locations are requested to be used for distributing specific VNFC, and such a deployment can only be inferred based on affinity/anti-affinity constraints processed by the NFVO.

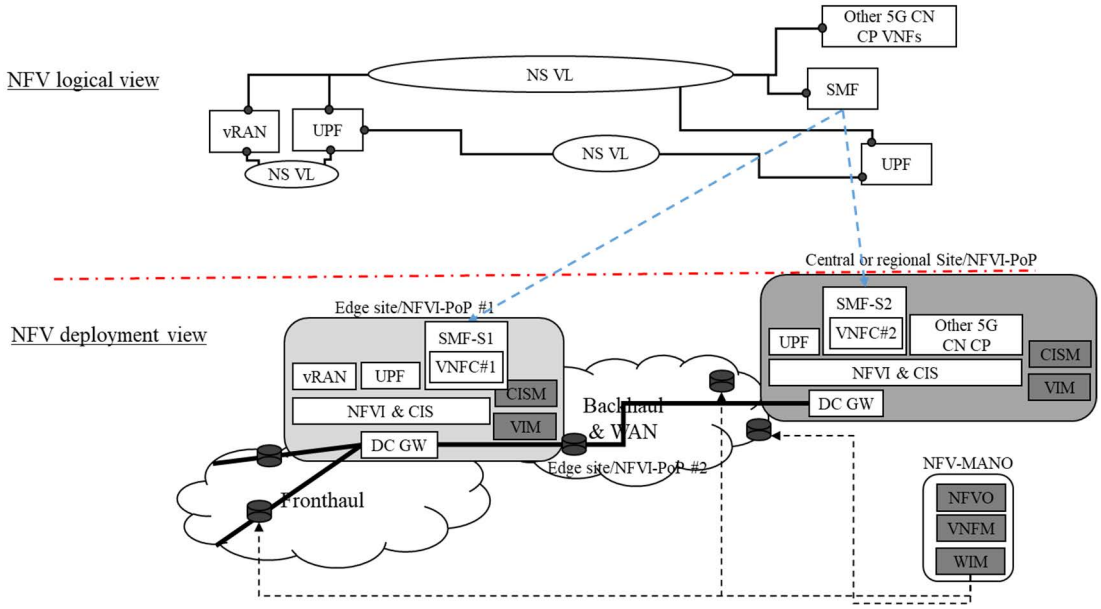


Figure 5.5.3.4-1: Example of distributed deployment of an NF

5.5.4 Gap analysis

The referred ETSI NFV specifications in the present characteristic profiling do not document:

Gap #4.1: It is not possible to provide to NFV-MANO location constraints at a granular level below VNF.

5.6 Characteristic #5: Unified authentication frameworks

5.6.1 Introduction

The 5GS "unified authentication framework" involves two aspects. From a 5G core network perspective, ETSI TS 123 501 [i.2] specifies that the 5G core network supports:

- UE authentication by network; and

- network slice specific authentication.

And from a perspective of securing the 5GS, ETSI TS 133 501 [i.14] specifies the security architecture supporting the authentication and authorization between network functions. In the case of UE authentication by network and network slicing specific authentication, the authentication is realized at the application layer. In this clause, UE authentication aspects are not investigated in detail.

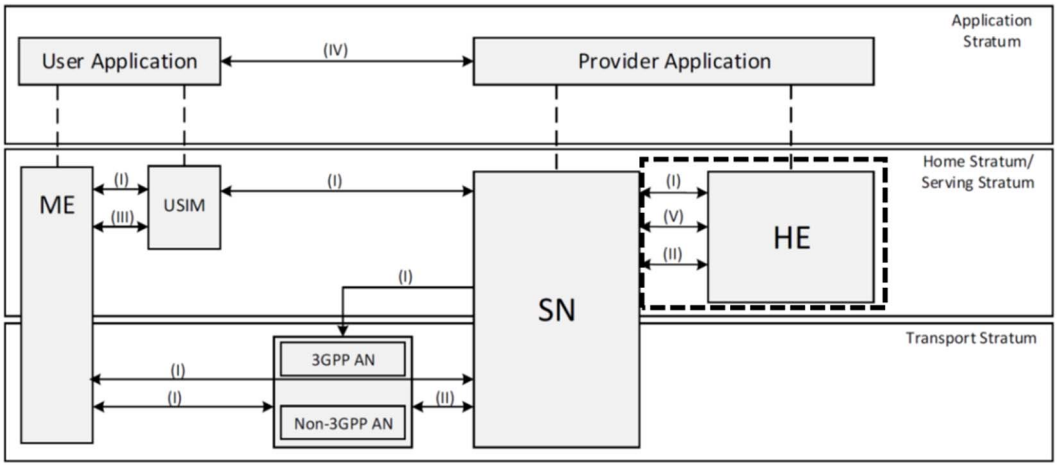


Figure 5.6.1-1: Overview of the security architecture (from ETSI TS 133 501 [i.14])

According to figure 5.6.1-1, following security domains are used:

- Network access security (I): The network authenticates the Subscription Permanent Identifier (SUPI) and the UE authenticates the serving network. The Access and Mobility Management function (AMF) includes access authentication and access authorization functionality.
- The serving network authorizes the UE based on authentication through the subscription profile obtained from the home network.
- Network domain security (II): Traditional EPS based communication.
- Application domain security (IV): In Network Slice-Specific Authentication and Authorization, AMF invokes an EAP-based Network Slice-Specific Authentication and Authorization after network authentication and authorization.
- SBA domain security (V): All network functions support mutually authenticated TLS and HTTPS. Authentication is implemented with credential. The OAuth 2.0 based authorization framework is mandated for NRF and NF according to ETSI TS 133 501 [i.14].

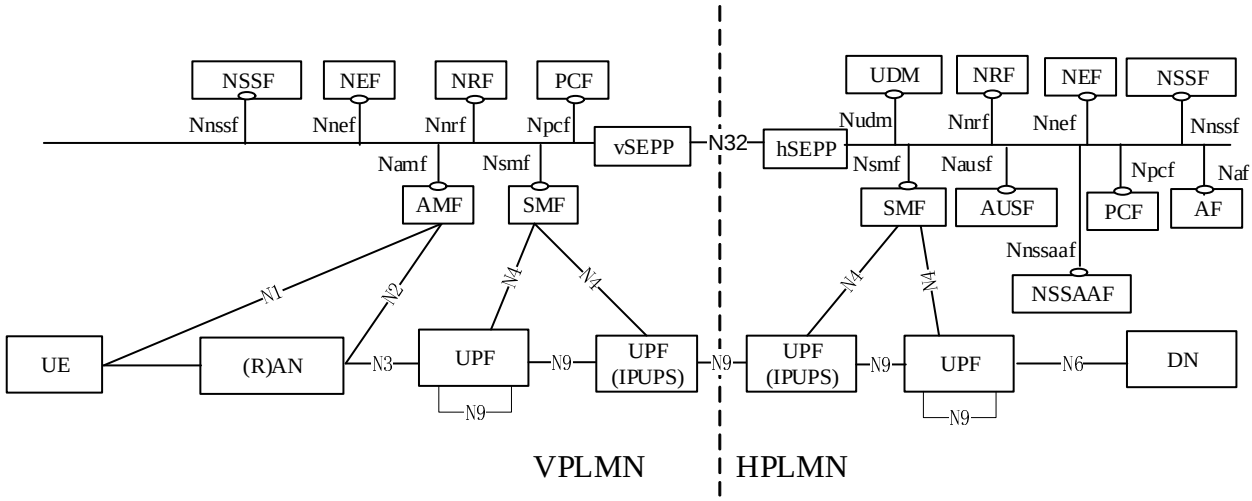


Figure 5.6.1-2: Roaming 5G System architecture (from ETSI TS 123 501 [i.2])

According to figure 5.6.1-2, the 5G System architecture introduces a Security Edge Protection Proxy (SEPP) and Inter-PLMN UP Security (IPUPS) as an entity sitting at the perimeter of the PLMN for protecting control plane messages and user plane messages, as specified in ETSI TS 133 501 [i.14]:

- SEPP: the SEPPs use JSON Web Encryption for protecting messages on the N32 interface as application layer.
- IPUPS: the IPUPS use standardized solution for binding 5G SBA REST Service Operations between SMFs to GTP-U over N9 in roaming scenarios.

Authentication and authorization between network functions in SBA domain security (V) and over N32 via SEPPs use two types of framework according to ETSI TS 133 501 [i.14]:

- Authentication and static authorization: static authorization is based on local authorization policy at the NRF, and authentication is mutually authenticated TLS and HTTPS.
- OAuth 2.0 based authorization: NRF is the OAuth 2.0 authorization server and network function is OAuth 2.0 client or resource server, and authentication is mutually authenticated TLS and HTTPS. However, no resource owner is defined for OAuth2.0 in the referred 3GPP specification. Figure 5.6.1-3 illustrates an overview of the OAuth 2.0 framework.

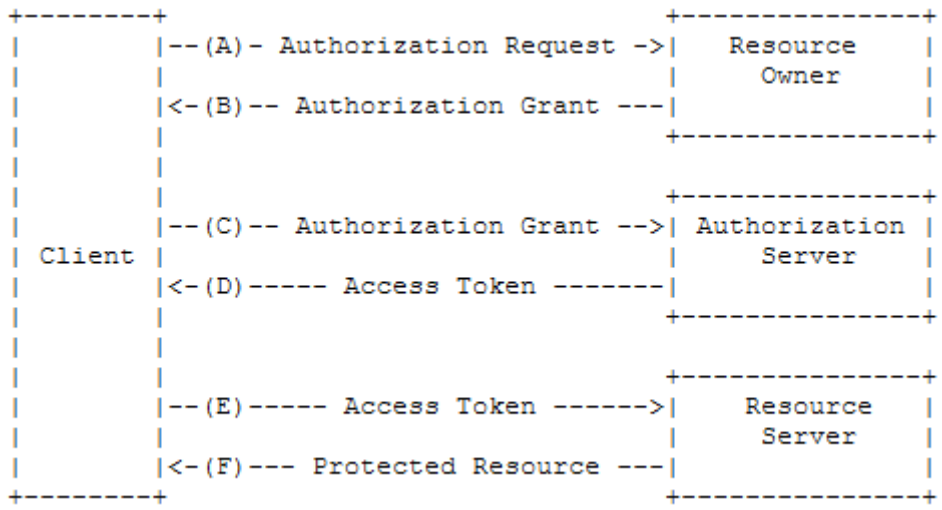


Figure 5.6.1-3: Overview of OAuth 2.0 framework (from IETF RFC 6749 [i.17])

Before step (C) in figure 5.6.1-3, and as a pre-condition, the resource server registers information to the authorization server. According to clause 5.2.2.2.2 of ETSI TS 129 510 [i.33], the resource server as NF service consumer of NRF sends a PUT request to the authorization server in NRF. Then the NRF returns "201 Created" on success, or "400 Bad Request" on NRF internal error, or some 3xx status code to indicate redirection as described in figure 5.6.1-4.

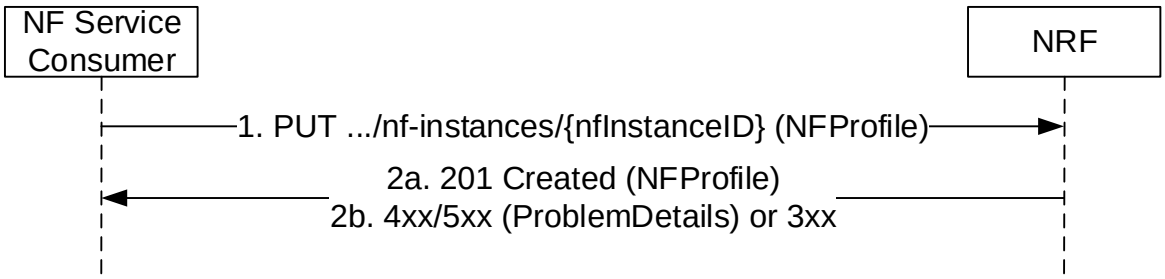


Figure 5.6.1-4: NF registration to NRF (from ETSI TS 129 510 [i.33])

5.6.2 Profiling of related NFV capabilities, features and specifications

5.6.2.1 General NFV concepts

No general NFV concept is applicable for the present characteristic profiling.

5.6.2.2 Specific profiling aspects and specification references

ETSI GR NFV-SEC 005 [i.34] introduces relevant security-related elements for authentication and authorization which are relevant for the present characteristic profiling:

- Certificate.
- Credential.
- Certifiate Authority (CA).

Other security-related elements of relevance, but not explicitly documented in ETSI GR NFV-SEC 005 [i.34] are:

- Resource owner.
- Access Control List (ACL).

Clause 8.1.1.1.1 of ETSI GR NFV-SEC 005 [i.34] describes how NFVI generates a key-pair and the key-pair is shared with the VNF instance via the VNFM, as described in figure 5.6.2.2-1.

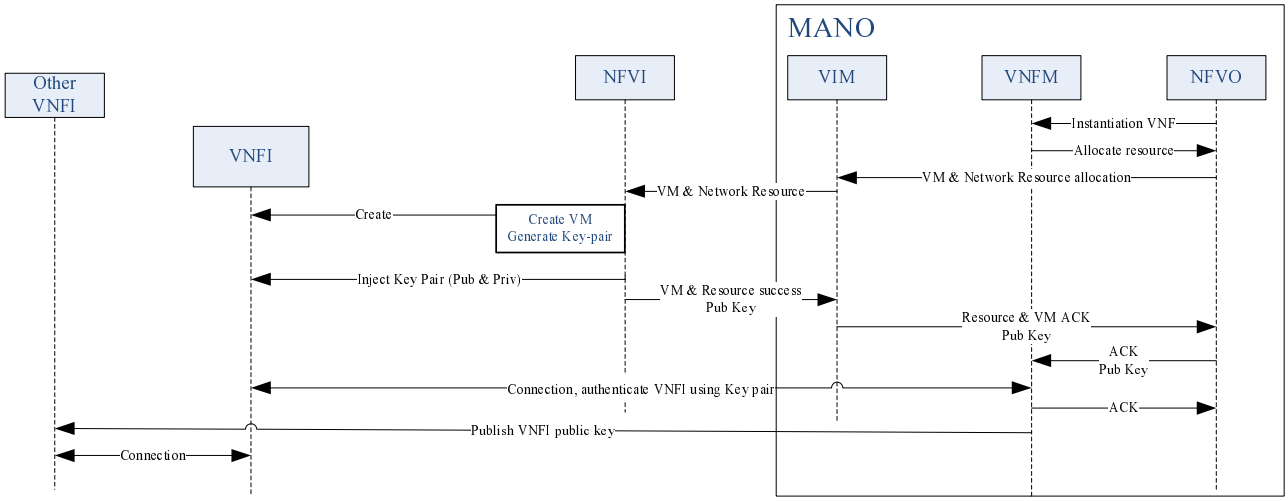


Figure 5.6.2.2-1: NFVI generate key pair procedure (from ETSI GR NFV-SEC 005 [i.34])

An example using Enrolment over Secure Transport (EST) is provided in figure 5.6.2.2-2, but other certificate protocols could be used following the recommendations from ETSI GR NFV-SEC 005 [i.34]. A certificate request is sent to the EST server, the CA creates a certificate and then the certificate is shared to the VNFC instance. This procedure is illustrated in figure 5.6.2.2-2. Note that the EST service could be merged with RA/CA. In relation to step-1 and step-2 in figure 5.6.2.2-2, this enrolment procedure assumes there is a day-0 certificate installed in the VNFC at the VNFC instantiation.

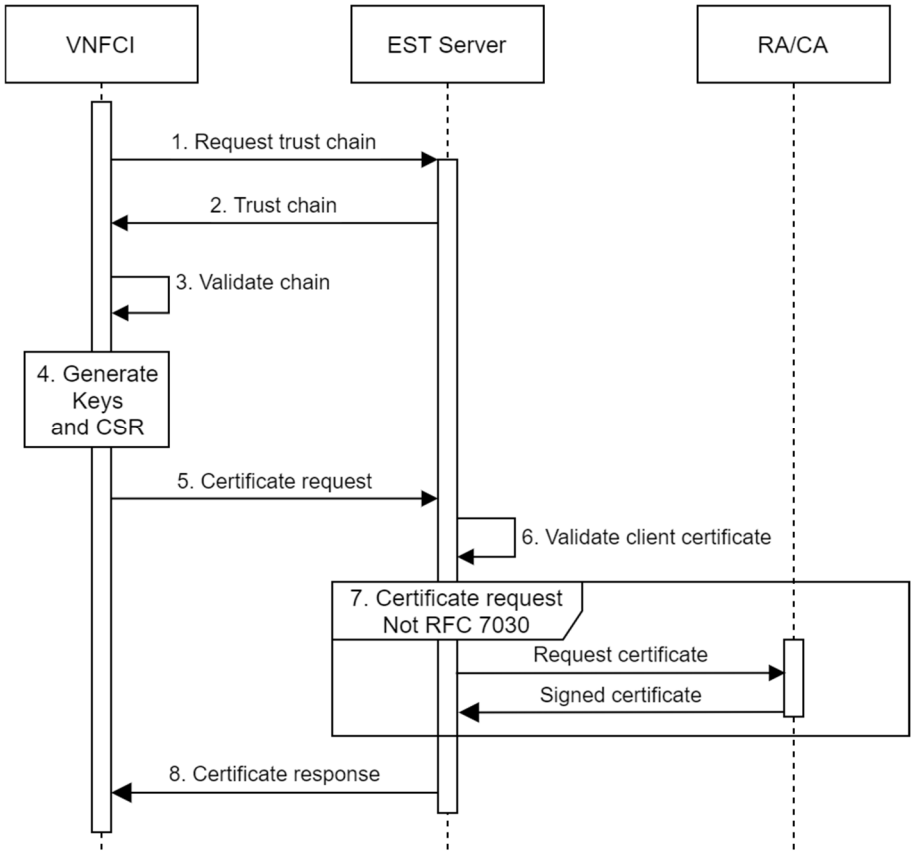


Figure 5.6.2.2-2: Direct VNFC instance certificate enrolment procedure (from ETSI GR NFV-SEC 005 [i.34])

5.6.3 Potential solutions

5.6.3.1 Solution #5A: CA server and Resource owner as VNFs

5.6.3.1.1 Overview

In this solution set, VNFs implement CA server functionality and Resource owner aspects, while ACL, and Certificates, Credentials are managed security objects either exchanged or used by these functions, as illustrated in figure 5.6.3.1.1-1. The authentication and authorization are implemented in the 3GPP application layer. Therefore, NFV-MANO is not involved in the authorization and authentication procedures.

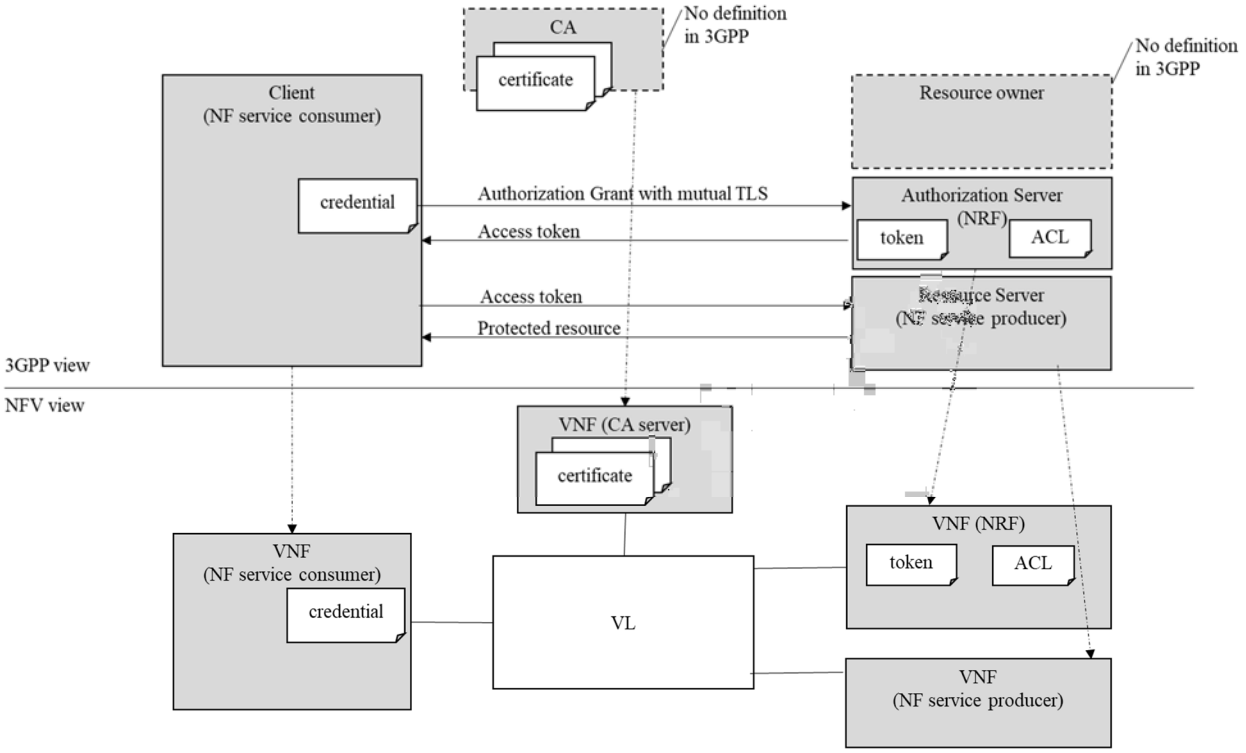


Figure 5.6.3.1-1: Mapping of 3GPP entities to NFV model

5.6.3.1.2 Solution #5A-A: Provisioning credential to VNFC instance as described in ETSI GR NFV-SEC 005

In this solution, TLS communication between NF service consumer and NRF uses certificates signed by the network operator as CA as described in ETSI GR NFV-SEC 005 [i.34]. NF service consumer and NRF are able to trust each other and connect with mutual TLS to authenticate. NF service consumer registers to NRF as described in clause 5.2.2.2.2 of ETSI TS 129 510 [i.33]. NF service consumer is authenticated and authorized by the NRF.

5.6.3.1.3 Solution #5A-B: Use of preconfigured certificate

In this solution, it is assumed that TLS communication between NF service consumer and NRF uses a preconfigured certificate in each of the entities, which different CAs might sign. These certificates are assumed not to be trusted, and mutual TLS communication cannot be established between NF service consumer and NRF. In such a case, any NF service consumer, including unauthorized application, cannot register to the NRF. As the NRF's access restriction for the consumers cannot be provided via mechanisms at the application layer, NFV-MANO can support access restriction for NF service consumer registration via the configuration of necessary security groups. After that, NF service consumer registers to NRF as described in clause 5.2.2.2.2 of ETSI TS 129 510 [i.33]. NF service consumer is authenticated and authorized by the NRF.

5.6.3.2 Solution #5B: CA server as VNF, NFV-MANO manages Resource owner, ACL, Certificates, Credentials

In this solution, VNFs implement CA server functionality and NFV-MANO manages Resource owner, ACL, certificates and credentials as illustrated in figure 5.6.3.2-1. NRF can be a VNF Common Service function as introduced by ETSI GR NFV-IFA 029 [i.16]. In this solution, the authentication and authorization procedures are implemented in the 3GPP application layer, but NFV-MANO is leveraged for setting up the security bindings for authentication and authorization based on the VNF and NS LCM orchestration.

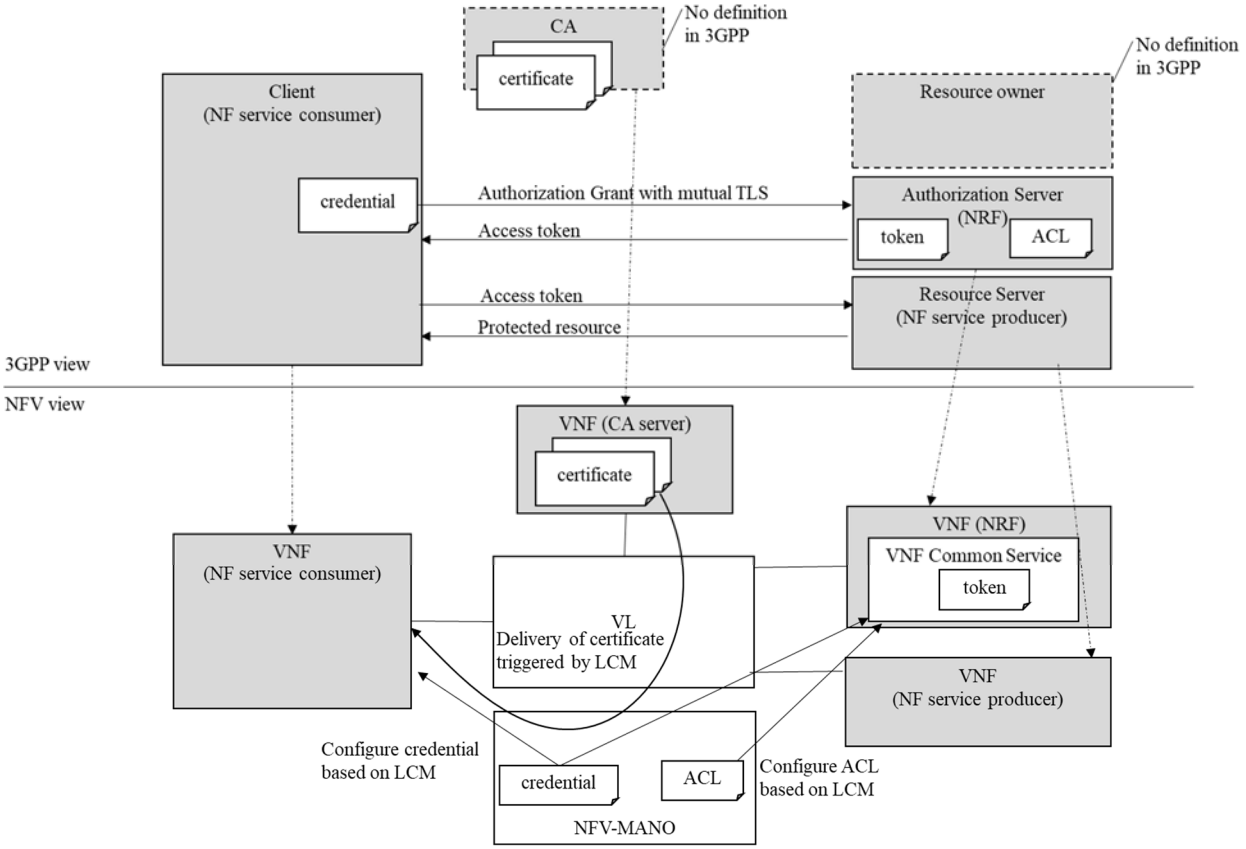


Figure 5.6.3.2-1: Mapping of 3GPP entities to NFV model

NFV-MANO configures credential and certificate to the VNF acting as an NF service consumer through the VNF Configuration interface specified in ETSI GS NFV-IFA 008 [i.18] or userData in Virtualised Compute interface specified in ETSI GS NFV-IFA 006 [i.19] after getting the certificate from the CA server (which is deployed as a VNF), as described in ETSI GR NFV-SEC 005 [i.34]. During the LCM of the VNF acting as NF service consumer, NFV-MANO registers the credentials and necessary ACL information to the NRF which is deployed as a VNF and has OAuth authorization server functionality deployed as a VNF Common Service function.

5.6.3.3 Solution #5C: NFV-MANO manages CA server, Resource owner, ACL, Certificates, Credentials

In this solution, NFV-MANO manages CA server functionality, Resource owner, ACL, certificates and credentials as illustrated in figure 5.6.3.3-1. NRF and CA server can be deployed as VNF using VNF Common Service function that deliver authorization server and CA server functionality, respectively. In this solution, the authentication and authorization procedures are implemented in the 3GPP application layer, but NFV-MANO is leveraged for setting up the security bindings for authentication and authorization based on the VNF and NS LCM orchestration.

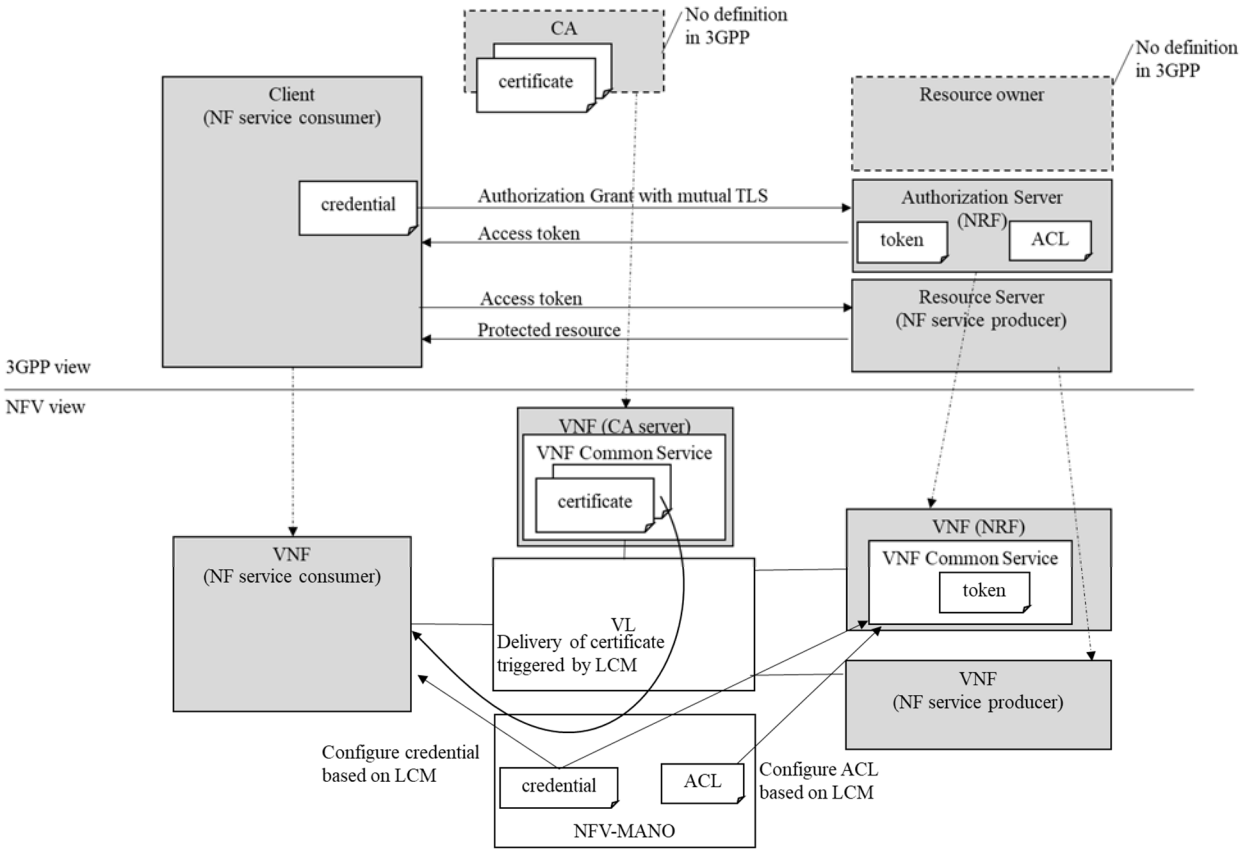


Figure 5.6.3.3-1: Entity mapping of 3GPP entities to NFV model

NFV-MANO configure credential and certificate to the VNF acting as NF service consumer through the VNF Configuration interface specified in ETSI GS NFV-IFA 008 [i.18] or userData in Virtualised Compute interface specified in ETSI GS NFV-IFA 006 [i.19] after getting the certificate from CA server (which is deployed as a VNF using a VNF Common Service delivering such CA server functionality), as described in ETSI GR NFV-SEC 005 [i.34]. During the LCM of the VNF acting as an NF service consumer, NFV-MANO registers the credentials and necessary ACL information to the NRF, which is deployed as a VNF and has OAuth authorization server functionality deployed as a VNF Common Service function.

5.6.4 Gap analysis

The referred ETSI NFV specifications in the present characteristic profiling and document do not specify:

Gap #5.1: In relation to potential Solution #5A-B, current NSD support defining security group rules at the NS level to enable NFV-MANO to support configuring security groups of designated CPs of a VNF dynamically based on LCM of other VNF.

Gap #5.2: In relation to potential Solution #5B and #5C, NFV-MANO support to provision and manage authorization server as VNF Common/Dedicated Service function.

Gap #5.3: In relation to potential Solution #5C, NFV-MANO support to provision and manage CA as VNF Common/Dedicated Service function.

Gap #5.4: In relation to potential Solution #5B and #5C, NFV-MANO to register new VnfExtCPs and unregister old VnfExtCps into the ACL of the authorization server during corresponding LCM.

Gap #5.5: In potential solution #5A-A and to cope with the impracticability of solution #5A-B, there is a need to bind the PKI LCM and more specifically the certificate LCM with the VNF/VNFC LCM.

5.7 Characteristic #6: Stateless NF, with separation of data processing from state

5.7.1 Introduction

ETSI TS 123 501 [i.2] specifies the 5G system supporting "stateless" NFs, where the "compute" resource is decoupled from the "storage" resource for distributed, redundant, stateless, and scalable NF instance as one of key principles and concept. Figure 5.7.1-1 depicts the data storage architecture for unstructured data from any NF as defined in ETSI TS 123 501 [i.2]. The 5G system architecture allows any NF to store and retrieve its unstructured data into/from a Unstructure Data Storage Function (UDSF).

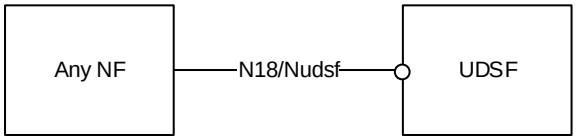


Figure 5.7.1-1: Data storage architecture for unstructured data from any NF (from ETSI TS 123 501 [i.2])

Figure 5.7.1-2 illustrates the data storage architecture that allows the Unified Data Management (UDM), Policy Control Function (PCF) and Network Exposure Function (NEF) to store data in the Unified Data Repository (UDR), as supported by the 5G system architecture.

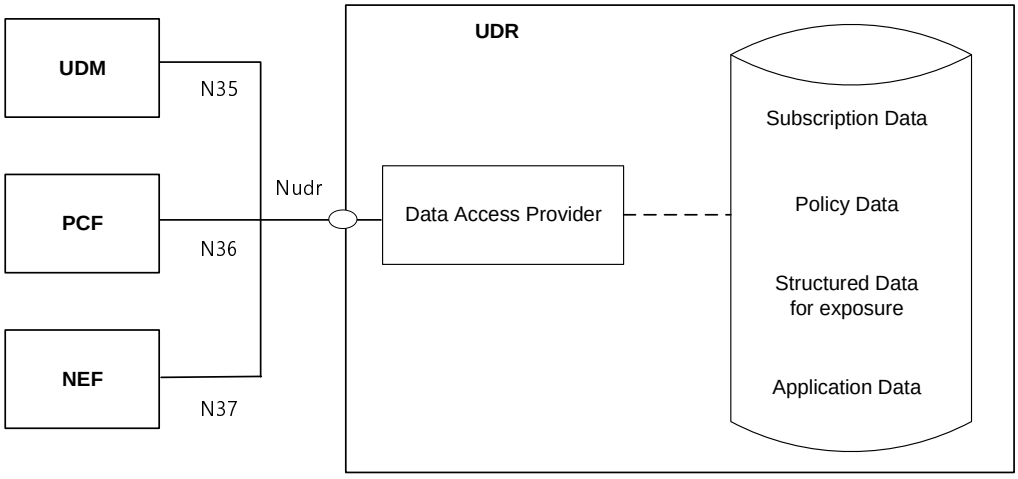


Figure 5.7.1-2: Data storage architecture (from ETSI TS 123 501 [i.2])

The content and format/encoding of operator specific data and operator specific data sets are not subject to standardization in ETSI TS 123 501 [i.2]. Other data such as subscription data, policy data, structure data for exposure and application data such as packet flow descriptions are subject to standardization. UDR and UDSF and other stateful NFs are the entities that hold state.

NOTE: According to ETSI TS 123 501 [i.2], structured data is referred to data for which the structure is defined in 3GPP specifications, and unstructured data for data for which the structure is not defined in 3GPP specifications.

According to ETSI TS 123 501 [i.2] AMF has access authentication functionality and has the capability of holding state of mid-term lifetime data. Also SMF has session management and has the capability of holding state of mid-term lifetime data.

5.7.2 Profiling of related NFV capabilities, features and specifications

5.7.2.1 General NFV concepts

The NFV information and data modelling provides the following capabilities to support "stateless" NFs:

- distributed: multi-site connectivity;
- redundant: affinity/anti-afinity rule for VNFC level and VNF level;
- stateless: management of individual and decoupled virtual storage resources;
- scalable NF instance: on-demand and auto-scaling.

NFV supports scaling of a VNF by using the concept of "scaling aspects". In complex VNF designs, scaling a VNF often involves adding/removing a number of related VNFC instances of several different types, possibly based on multiple VDUs. Depending on the VNF design, scaling aspects can refer to specific properties of the VNF such as being associated to a particular VNFC based on a specific VDU, which enables the consumer to perform scaling at the VNFC level.

In order to structure the functionality and increase the scalability and reliability of the VNF, separation of components realizing different functionality in the VNF is of great importance. In particular, regarding stateful vs. stateless VNF, this translates into separating stateless VNFC from VNFC that keep state. By using the "scaling aspects" capability, consumers and NFV-MANO can then manage stateless VNFC via the VNF LCM.

Figure 5.7.2.1-1 shows the Mapping of 3GPP and NFV view of holding state.

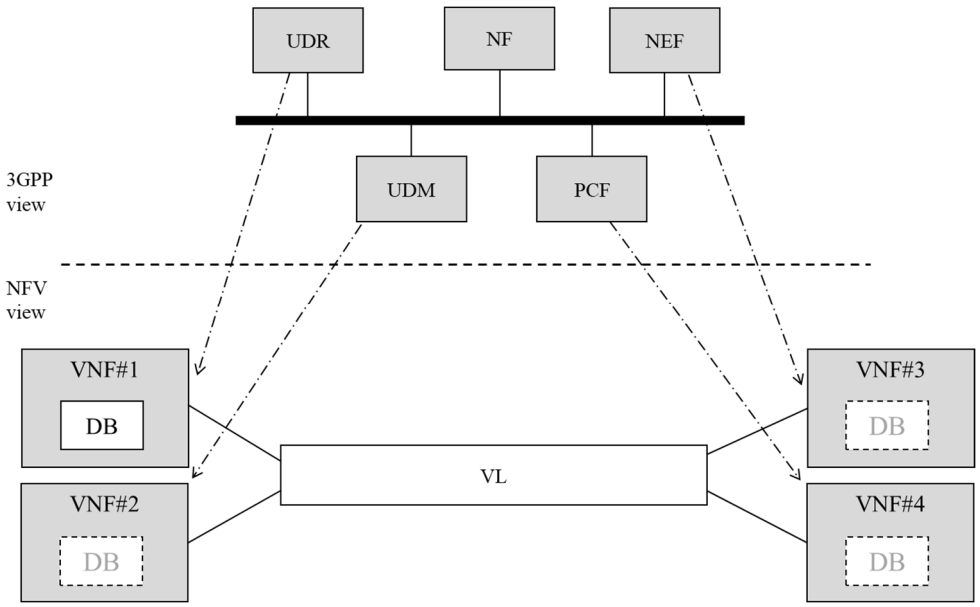


Figure 5.7.2.1-1: Mapping of 3GPP and NFV view of holding state separated at NF level

Figure 5.7.2.1-2 shows an example of separating state and stateless components at the NF level.

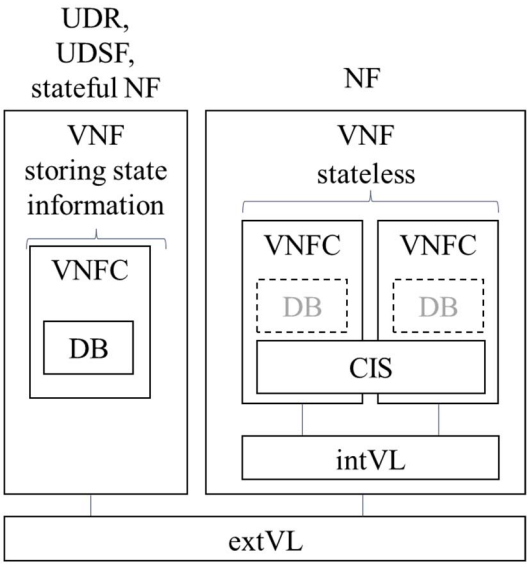


Figure 5.7.2.1-2: Example of NF level state and stateless composition

5.7.2.2 Specific profiling aspects and specification references

The VNFD of a VNF, whose information model and requirements are specified in ETSI GS NFV-IFA 011 [i.12], supports the specification of persistent and ephemeral storage for a VNF. The persistent virtual storage resources for a VNF are described by the "VirtualStorageDesc" information element. The ephemeral virtual storage specification depends on the type of virtualisation container:

- For a virtual machine, the "VirtualComputeDesc" information element is used.
- For an OS container, the "OsContainerDesc" information element is used instead.

Different types of persistent storage can be defined, namely: block, object and file-based storage. Depending on the type of storage, additional capabilities such as support for RDMA, file system protocols, etc. can also be defined, together with the size of the storage. In addition, the "VirtualStorageDesc" supports defining whether the virtual storage resource to be instantiated is per VNFC instance, and whether the lifetime of the storage is or not independent from the individual VNFC based on the VDU that refers such storage requirement.

Regarding the ephemeral storage in the case of VM-based VNFC, the ephemeral disks can be of block-type storage as defined by the corresponding "virtualDisk" attribute of the "VirtualComputeDesc". Zero or more virtual disks can be associated to a VM.

The ephemeral storage for the VNFC based on OS containers is defined via the "OsContainerDesc". As offered by underlying container management and orchestration solutions, both requested and limits for ephemeral storage associated to an OS container can be defined.

Annex C of ETSI GS NFV-IFA 011 [i.12] provides additional information and examples about the implementation of ephemeral storage for a VNF.

5.7.3 Potential solutions

5.7.3.1 Solution #6A: Dedicated VNF or VNFC for keeping state

5.7.3.1.1 Overview

In this solution set, a VNF or VNFC is responsible for keeping state.

5.7.3.1.2 Solution #6A-1: VNFC using virtual storage for keeping state

In this solution, a VM-based VNFC attaches to virtual storage and container-based VNFCs consume VM-based VNFC's storage via internal VL. Figure 5.7.3.1.2-1 illustrates an example of VNFC using virtual storage for keeping state.

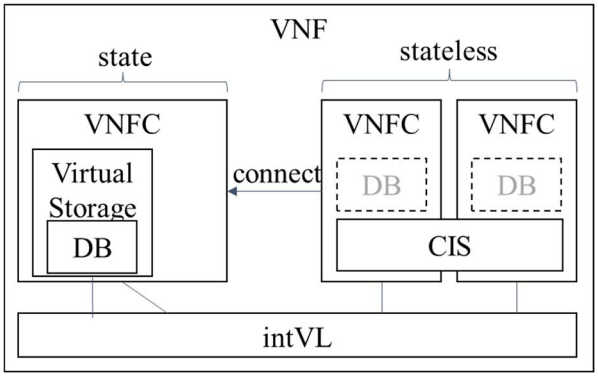


Figure 5.7.3.1.2-1: Example of VNFC using virtual storage for keeping state

5.7.3.1.3 Solution #6A-2: Dedicated VNF keeping state

In this solution, container-based VNFs use dedicated VNF like UDR specified in 3GPP for keeping state. Figure 5.7.3.1.3-1 illustrates an example of VNF using dedicated VNF for keeping state.

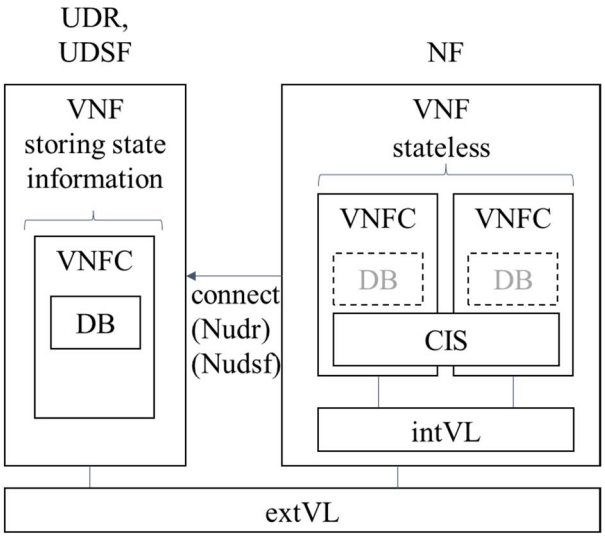


Figure 5.7.3.1.3-1: Example of dedicated VNF keeping state

5.7.3.2 Solution #6B: VNF Common Function for state

In this solution, container-based VNFCs use a VNF Common Service DB, as introduced by ETSI GR NFV-IFA 029 [i.16]. Figure 5.7.3.2-1 illustrates an example of "Common Function" for keeping state.

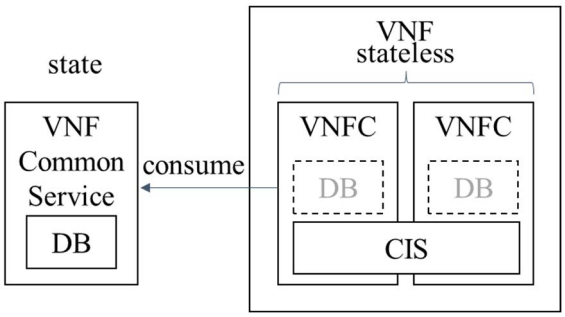


Figure 5.7.3.2-1: Example of VNFC using "VNF Common Service" for keeping state

5.7.3.3 Solution #6C: CIS using virtual storage for state

In this solution, container-based VNFCs use CIS's virtual storage directly via internal VL. Figure 5.7.3.3-1 illustrates an example of CIS providing virtual storage for keeping state.

NOTE 1: Use of internal VL in the present solution and in the referred figure is for illustrative purposes since the definition of internal VL in container-based VNF depends on the type of cluster networks such as primary vs. secondary internal cluster networks.

NOTE 2: Despite not being illustrated in the present clause, a very similar solution is also possible for the VM-based VNFCs, wherein the virtual storage is provided by the NFVI's storage resources.

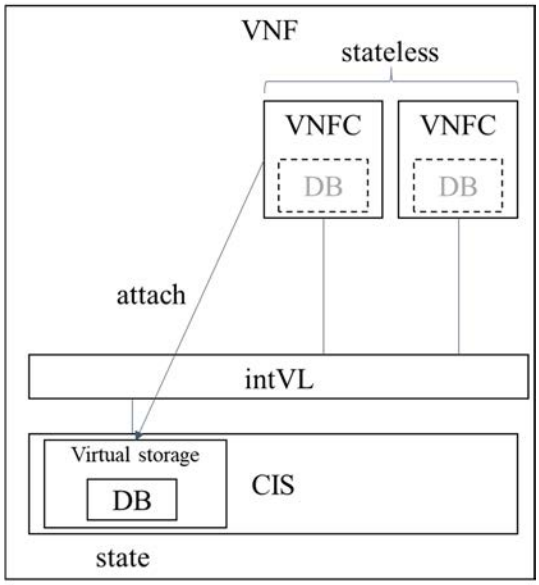


Figure 5.7.3.3-1: Example of CIS providing virtual storage for keeping state

5.7.4 Gap analysis

The referred ETSI NFV specifications in the present characteristic profiling do not document:

Gap #6.1: In the case of persistent storage, it is not possible to scale virtual storage resources independently from the associated VNFC, since the scaling aspects of a VNF only support horizontal scaling of VNFC instances, adding or removing bitrate to VLs and VIP CP instances.

Gap #6.2: As per Solutions #6B and #6C, virtual storage can be shared and used a common resource among different VNF, and it currently not possible to indicate in the referred specification how a VNF is expected to reuse shared storage.

5.8 Characteristic #7: Network capabilities exposure

5.8.1 Introduction

A key component of the 5GCN is the Network Exposure Function (NEF) which enables external Application Functions (AFs) to interact with the 5GS and expose capability of the 5G network. The external exposure capabilities are further sub-categorized, including monitoring, provisioning, policy/charging and analytics.

Trusted AFs can interact directly with the 5GS, whereas untrusted AFs communicate through the NEF. NEF is the successor of SCEF in 4G, while a trust domain for NEF is same as trust domain for SCEF as defined in ETSI TS 123 682 [i.22]. An AF can get services from multiple NEFs, while a NEF can provide service to multiple AFs, as illustrated in figure 5.8.1-1.

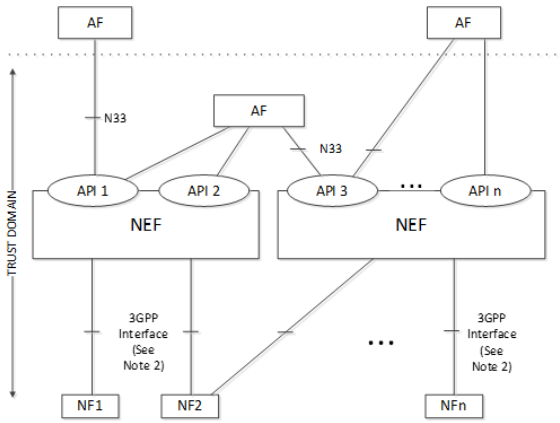


Figure 5.8.1-1: Non-roaming architecture for Network Exposure Function in reference point representation (from ETSI TS 123 501, figure 4.2.3-5 [i.2])

The overall NEF architecture is presented in ETSI TS 123 502 [i.8], clause 4.15. When an NEF is used for external exposure, the Common API Framework for 3GPP northbound APIs (CAPIF) and associated API provider domain functions can be supported, as specified in ETSI TS 123 222 [i.23]:

- NEF northbound: The NEF northbound interface is specified by the N33 reference point. In more detail it specifies RESTful APIs that allow the AF to access the services and capabilities provided by 3GPP network entities and exposed securely by NEF. For the NEF northbound interface, stage 2 level requirements and signalling flows are defined in ETSI TS 123 502 [i.8] and stage 3 solutions in ETSI TS 129 522 [i.24].
- NEF southbound: NEF interacts with different Network Functions (NFs) residing in the 5GC through the corresponding southbound interfaces. For example, N29 is the interface between NEF and SMF, N30 is the interface between NEF and PCF, and N52 is the interface between NEF and UDM.

NEF Functionality

The NEF supports one or more of the functionalities described below (refer to ETSI TS 123 501 [i.2]):

- Exposure of capabilities and events for 3rd party, AFs, Edge Computing.
- Secure provision of information from external application to 3GPP network, like expected UE Behaviour, 5G-VN group information and service specific information.
- Translates the information received from the AF to the one sent to internal 3GPP NFs, and vice versa.
- Interacts with other 5GS NFs and stores the received information as structured data using a standardized interface to UDR. The stored information can be accessed and "re-exposed" by the NEF to other network functions and AFs.
- An NEF can also support a Packet Flow Description (PFD) Function to store and retrieve PFD(s) in the UDR and provide PFD(s) to the SMF (pull mode or push mode), as described in ETSI TS 123 503 [i.25].

- Support of 5G-VN Group Management Function. For example, the NEF exposes a set of services to manage (e.g. add/delete/modify) 5G-VN groups and 5G VN members.

- Used for analytics exposure. NWDAF analytics can be securely exposed by NEF for external party, as specified in ETSI TS 123 288 [i.26].

- Retrieval of data from external party by NWDAF. Data provided by the external party can be collected by NWDAF via NEF for analytics generation purpose. The details for the data collected from an AF as well as interactions between NEF, AF and NWDAF are described in ETSI TS 123 288 [i.26].

- Additional functionality is also supported, like support of Non-IP Data Delivery (NIDD), management of NIDD configuration and delivery of Mobile Originated (MO) and Mobile Terminated (MT) unstructured data, charging data collection and support of charging interfaces.

NEF Registration and discovery

A 5G NF can either use a locally configured NEF instance or discover one from NRF, which is used to provide profile(s) of NEF instance(s) to NFs customers. Several factors can affect the NEF selection like slice identification and AF identification (refer to clause 6.3.14 of ETSI TS 123 501 [i.2]). To use the NEF services, AF is expected to be aware of the NEF API Gateway Service URL (FQDN) and/or the API Gateway service IP address (v4 or v6).

NEF connectivity information can be provided to AF via three possible ways:

- The IP address(es)/port(s) of the NEF are locally configured in the AF.

- AF can discover the FQDN or IP address(es)/port(s) of the NEF by performing a DNS query using the External Identifier of an individual UE (or using the External Group Identifier of a group of UEs).

- If the AF is trusted by the operator, the AF can query the NRF to discover the FQDN or IP address(es)/port(s) of the NEF.

Service Exposure for EPC-5GC Interworking

In scenarios where interworking between 5GS and Evolved Packet Core (EPC) is possible, the network configuration is expected to associate UEs with SCEF+NEF node(s) for Service Capability Exposure. The SCEF+NEF hides the underlying 3GPP network topology from the AF (e.g. SCS/AS) and hides whether the UE is served by 5GC or EPC. The SCEF+NEF uses only 5GC procedures to configure monitoring events in EPC and 5GC and in terms of the CAPIF, the SCEF+NEF is considered a single node. Common state information is maintained by the combined SCEF+NEF node like SCEF+NEF ID (being the same towards the AF) and SCEF+NEF common IP address and port number.

QoS and resource allocation because of AF/NEF interaction

An AF can influence the traffic for UEs which are under its control using the Nnef_TrafficInfluence NEF service defined in clause 5.2.6.7 of ETSI TS 123 502 [i.8]. To apply requests to create or update traffic made by AF to NEF, a parameter mapping with 5GC parameters occurs as described in clause 5.6.7 of ETSI TS 123 501 [i.2]. For example, regarding traffic routing an AF can send through NEF requests to influence SMF routeing decisions for traffic of Protocol Data Unit (PDU) Session. The AF requests can influence UPF (re)selection and allow routeing user traffic to a local access to a Data Network (identified by a DNAI). The AF requests that target existing or future PDU Sessions of multiple UE(s) or of any UE are sent via the NEF and can target multiple PCF(s). The PCF(s) transform(s) the AF requests into policies that apply to PDU Sessions.

In principle in a virtualised context, this specific ability of NEF to expose such functionality to multiple AFs, could affect the resource allocation made by VIM, CISM and WIM to support the performance needed by specific VNFs and on per slice basis.

5.8.2 Profiling of related NFV capabilities, features and specifications

5.8.2.1 General NFV concepts

Descriptors

The Network Service Descriptor (NSD) defined in ETSI GS NFV-IFA 014 [i.9] is a deployment template used by the NFV-MANO to deploy an NS instance. It includes or references the descriptors of its constituent objects like VNFDs (defined in ETSI GS NFV-IFA 011 [i.12]), PNFDs, nested NSD; VLDs used by the NFVO to deploy Virtual Links (VL), and VNFFGDs.

Connection points and Service Access Points

Connection point (CP): represents the virtual and/or physical interface that offers the network connections between instances of NS, VNF, VNFC, PNF and a VL. According to ETSI GS NFV-IFA 011 [i.12], the VNFD supports specifying metadata related to network addresses to be assigned to CPs. For example, the metadata for layer 3 network addresses can include IP address type, range, and allocation scheme.

Service Access Points (SAP): ETSI GS NFV-IFA 014 [i.9] defines an SAP as the connection point where an NS can be accessed. For an NS the SAPs are specified in the NSD using the Sapd information element.

In a VNFFGD, the Nfpd information element is used to associate traffic flow criteria to a list of descriptors associated to the CP and SAP to be visited by traffic flows matching these criteria.

Relevant to connectivity are also VLDs and a number of information elements; for example constituentCpdId describes a connection point on a VNF/PNF or a SAP which connects to virtual links, NsVirtualLinkConnectivity information element describes connection information between a connection point and an NS Virtual Link, the NsQoS information element specifies quality of service parameters applicable to a NS VL.

References to ETSI GS NFV-IFA 014 [i.9] and ETSI GS NFV-IFA 011 [i.12] are provided for more details. The descriptions provided in the other characteristics in the present document like Characteristic #2: Service-based interfaces, communication and service mesh, relevant to CP, SAPs and connectivity concepts in MANO, also apply for this characteristic.

5.8.2.2 Specific profiling aspects and specification references

When implementing the NEF as a VNF, several specific aspects can be considered.

Internal vs external communication

Regarding the functionality of NEF, on the one hand, the NEF represents the interface of the 5GS to the "external world" through its interaction with the AFs. On the other hand, it also interacts internally with several other 5G NF such as SMF and PCF, which can also be virtualised VNFs/NSs. However, the connectivity and security requirements can be different. Signalling flows for the NEF Northbound interface are defined in ETSI TS 123 502 [i.8] for setting up an AF session. In the case NEF is deployed as a VNF, NFV-MANO's VIM or CISM support to provide the right levels of QoS of the NEF to AF(s) connections, when for example a single virtualised NEF residing inside the trusted domain is serving multiple AFs residing either inside or outside the trusted domain.

Furthermore, if an NEF is connected to an AF, mutual authentication is expected between the NEF and AF, which is fulfilled by using TLS, according to ETSI TS 133 210 [i.20] for security profiles for TLS implementation and ETSI TS 133 310 [i.21] for certificate-based authentication profiles. After AF is authenticated, OAuth-based authorization mechanism is used according to IETF RFC 6749 [i.17]. In case AF resides inside the operator domain then NFV-MANO can be also involved in the authentication/authorization process as described in Solution #B, clause 5.6.3.2 and Solution #C, clause 5.6.3.3. of characteristic Unified authentication framework of the present document.

Since NEF provides services to several different entities, API Gateway service URL (FQDN), API Gateway service IP address (v4 or v6) are exposed through NRF or through static configuration on the consumer side like in AF. When deploying NEF as a VNF, certain connectivity information can also be part of the CPD and/or SAPD. This means that the information provided in the relevant descriptors (VNFD, NSD) at design time could affect the relevant API Gateway information to be exposed.

A careful IP address allocation is expected to be preserved to avoid inconsistency on the network namespaces used for each occasion. Some SAPs enable external access to relevant AFs, while other SAP are used to enable internal 5GS communication.

Regarding the NEF northbound interface, an AF can get services from multiple NEFs, while an NEF can provide service to multiple AFs. The communication between a NEF VNF/NS and multiple AFs can occur either by using the same SAP or a dedicated SAP per AF. This will affect the SAP design, the resource allocation made to support the NEF VNF and the relevant NSDs.

5G, 4G internetworking

ETSI TS 123 501 [i.2] allows the deployment of a combined SCEF-NEF exposure service which hides from AF whether the UE is served by 5GC or EPC. The SCEF+NEF uses only 5GC procedures to configure monitoring events in EPC and 5GC. In the southbound, the exposure service communicates with both the 5GC services and the EPC services. In the northbound, the exposure service covers a N33 interface which also supports T8 interface.

If at the same time a single exposure service also connects to native 5G AF, then a design choice of having multiple SAPs for the northbound connections can be also considered, like using a different SAP for 5G-AF and SAP for AS/AF. Also depending on the number of AFs each NEF instance serves, the appropriate resource allocation can be performed by NFV-MANO.

NEF operations drive resource allocation of VLs and VIM, WIM

Through the NEF Nnef_TrafficInfluence service, an AF can affect decision making for the traffic of individual UEs and groups of UEs, on issues like packet routing and which UPF to be selected. Also, regarding the communication between AF and NEF itself, tunable parameters exist like the maximum latency which identifies maximum delay acceptable for downlink data transfers.

The ability of NEF to expose such functionality to AFs can eventually affect the resource allocation made by the NFV-MANO, and more precisely, by the VIM, CISM and even WIM for the relevant virtualised VNFs/NSs supporting the 5GS. This resource allocation can be also tailored to a specific slice.

5.8.3 Potential solutions

5.8.3.1 Solution #7A: NEF as a VNF; 5G VNF composition supporting a single NS

In this primitive solution case, NEF is deployed as a VNF as part of an NS, offering the exposure service to multiple AFs. The SAPs defined are used for network exposure either corresponding to actual exposed NEF CP, or wired to the NEF CP using the capability to expose NS VL. Through them the AFs can consume the services offered by NEF. Figure 5.8.3.1-1 illustrates this solution.

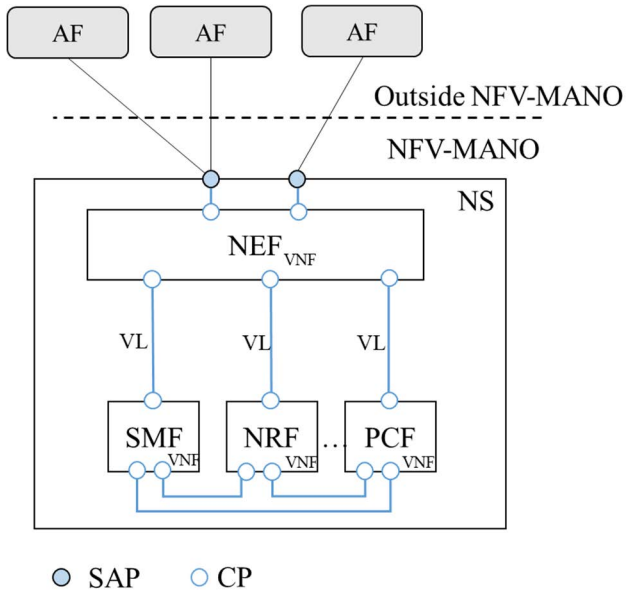


Figure 5.8.3.1-1: NEF as a VNF connected to multiple AFs

An AF can reside inside or outside the trust domain of the NEF. Also, in principle, AFs are outside the NFV-MANO control, however trusted AFs could be also virtualised and be part of the operator domain. For simplicity, the connection of the NS to other NSs that are building the overall 5GC is not depicted.

5.8.3.2 Solution #7B: Network Exposure with 4G/5G internetworking support

In this case the NS is again providing the network exposure service to external applications which could be either AFs (5G, N33 interface) or AS (4G, T8 interface) or both. Internally to the NS, a single VNF is used for network exposure supporting the functionality of both the SCEF and NEF. In the southbound this VNF is connected to both 5G VNFs and EPC VNFs (4G). Trust domain for NEF is same as Trust domain for SCEF as defined in ETSI TS 123 682 [i.22]. Figure 5.8.3.2-1 depicts this solution.

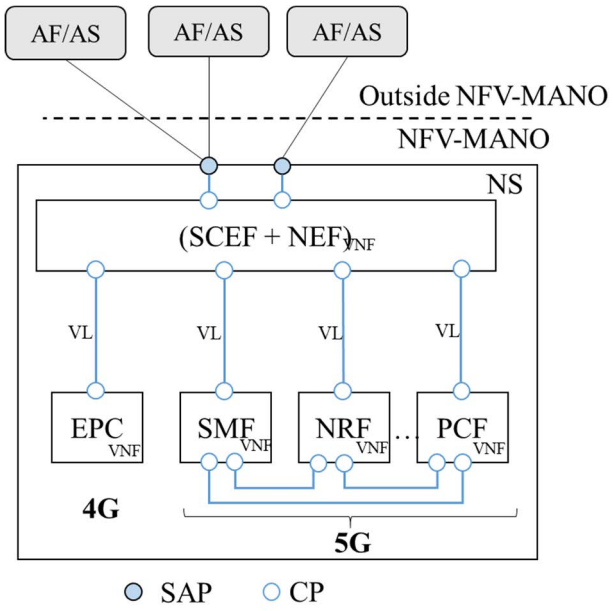


Figure 5.8.3.2-1: Network Exposure with 4G/5G internetworking support

Like in the previous case, an AF can reside inside or outside the trust domain of the SCEF-NEF. Also, in principle AFs are outside the NFV-MANO control, however trusted AFs could be also virtualised and be part of the operator domain.

5.8.3.3 Solution #7C: NEF VNF as part of a nested NS

A nested NS can be formed by a group of VNFs like in the previous solutions, or by a group of other NSs or combinations. In figure 5.8.3.3-1, the NS#3 exposes to AFs and/or AF/ASs the network exposure service through the appropriate SAPs. NS#3 is a composition of NS#1 supporting 5GC functionality, NS#2 supporting 4G services and a SCEF-NEF VNF offering the network exposure functionality. For simplicity, the connections of the NS to other NSs that are building the overall 5GC are not depicted.

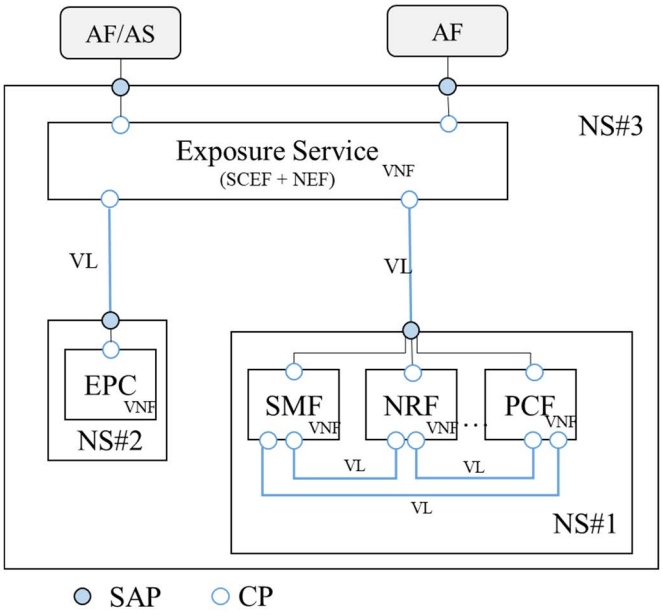


Figure 5.8.3.3-1: NEF VNF as part of a nested NS

5.8.4 Gap analysis

Communication requirements between NEF-VNF and AF reassemble similar properties like the ones of a firewall VNF as defined in ETSI GS NFV-SOL 006 [i.32], see Firewall Router Deployment, Annex A.2.2. For example, when considering the second scenario described in clause 5.8.3.2, where the NEF is exposed as a single independent NS, the traffic flow consists of external traffic that comes from AF to NEF-VNF over an SAP (described by corresponding SAPD as defined in ETSI GS NFV-IFA 014 [i.9]), which could be called "Outside" and realized as VNF external CP. The traffic exits the NEF-VNF using another CP called "Inside" into the 5GCN NS.

The referred ETSI NFV specifications in the present characteristic profiling do not document:

Gap #7.1: In case of communication pre-provisioning between NEF-NS and AF made by OSS, Gap #3.1 also applies, as defined in characteristic #3 Network slicing (clause 5.4.4).

Gap #7.2: As defined in the intro paragraph an "Outside" SAP can be used to enable connectivity between NEF-NS and AFs. However, an AF can be outside the trusted domain (ETSI TS 123 682 [i.22]) but can also reside inside the trusted domain and even be managed by NFV-MANO. This is the case for example where operator applications are exploiting the NEF services. In this case multiple "Outside" SAPs need to be provided (to support inside or outside the trusted domain AFs), based on a SAPD. In this regard, the support of "adding and removing SAP" as supported by ETSI GS NFV-IFA 013 [i.10] becomes relevant. The update NS operation specified in clause 7.3.5 by ETSI GS NFV-IFA 013 [i.10] supports the addition and removal of an SAP to/from an NS instance. However, how the action of adding/removing SAP translates into actual VNF and virtualised resource management is not fully defined, in particular when SAPs are mapped to VNF external connection points that are not subports. This also implies that current referred ETSI NFV specifications support CPs network isolation (i.e. different network segments) only via VLAN tagging in trunk mode, which might limit the modes of connectivity for the NEF services.

Gap #7.3: Current Cpd information element, from which the Sapd derives, is not able to support defining additional layer protocol data above L2 and L3 information, such as port number, as well as not able to qualify naming information, such as FQDN. Currently the definition of service properties of a connection point is only possible if the SAP is exposed by a VirtualCp acting as a VNF external SAP (see also clause 7.1.18 by ETSI GS NFV-IFA 011 [i.12]).

5.9 Characteristic #8: Roaming

5.9.1 Introduction

Following the capabilities supported in previous 3GPP mobile network generations to enable global and worldwide connectivity for users, 3GPP designed the 5G system with the principle of supporting roaming. As described in the ETSI TS 123 501 [i.2], the 5G system supports roaming in two scenarios:

- home routed traffic; and
- local breakout traffic in the visited PLMN (VPLMN).

In the local breakout scenario, the VPMLN handles the whole data plane traffic connectivity from the visiting UE to the Data Network (DN). In this case, the SMF and all UPFs involved in the PDU session are under control of the VPLMN. Figure 5.9.1-1 illustrates the local break roaming scenario.

In the home route scenario, the data plane traffic from the visiting UE is routed first through the VPLMN and then in the home PLMN (HPLMN) towards the DN. Thus, in this second scenario, the PDU session is supported by an SMF function under control of the HPLMN, by an SMF function under control of the VPLMN, and by at least one UPF under control of the HPMLN and by at least one UPF under control of the VPLMN. Figure 5.9.1-2 depicts the home routed roaming scenario.

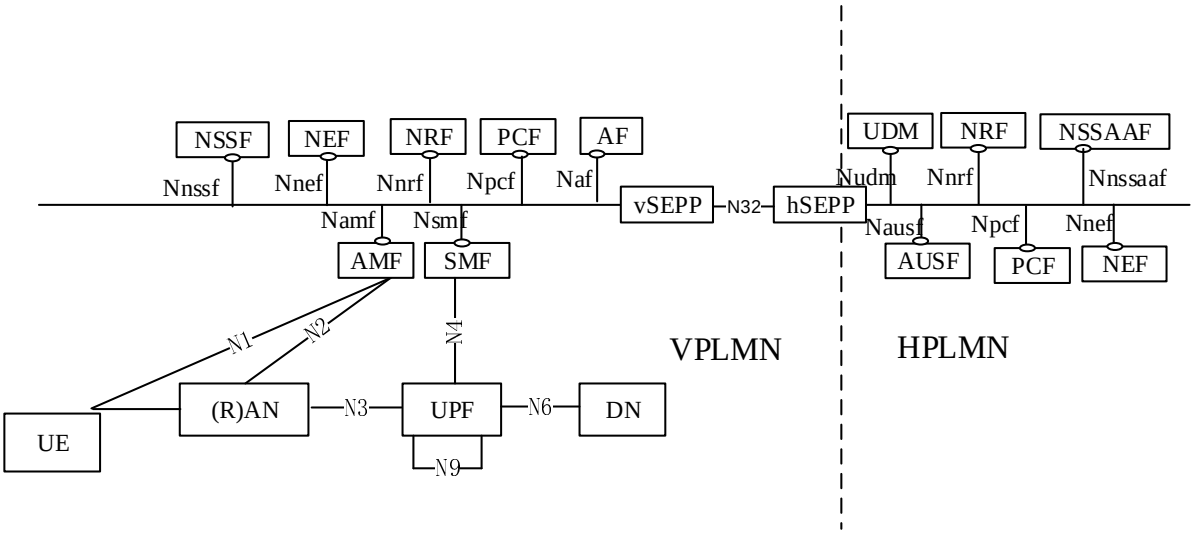


Figure 5.9.1-1: 5G system architecture of local breakout scenario in service-based interface representation (from ETSI TS 123 501 [i.2])

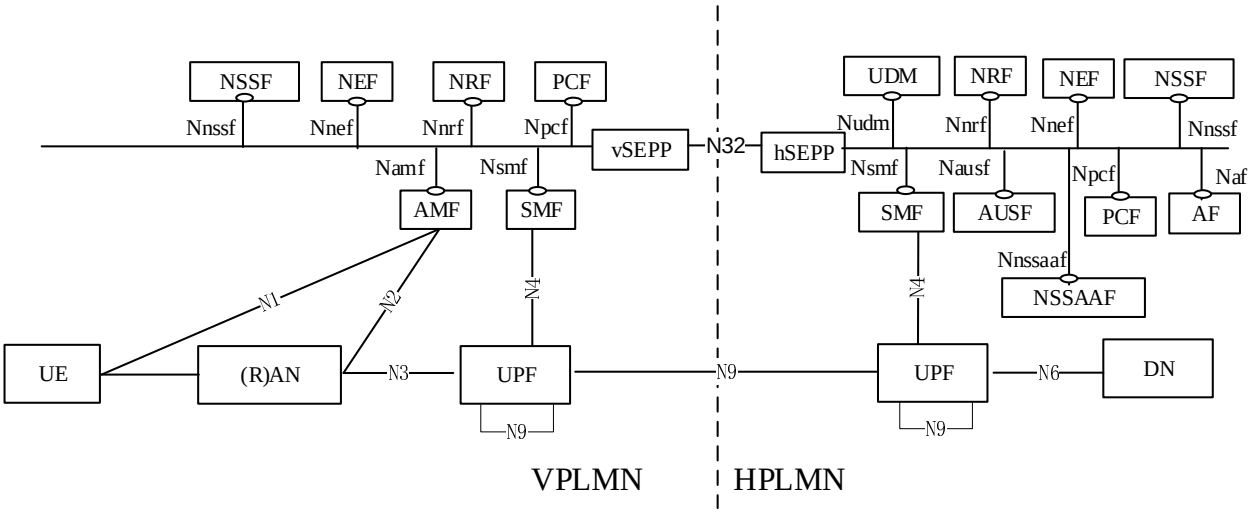


Figure 5.9.1-2: 5G system architecture of home routed scenario in service-based interface representation (from ETSI TS 123 501 [i.2])

The 5G system also supports that different simultaneous PDU sessions of a UE can use different modes: home routed and local breakout.

ETSI TS 123 501 [i.2] also contains 5G system roaming architecture in reference point representations. The same technical specification also provides architecture illustrations for the local breakout and home routed roaming scenarios for untrusted non-3GPP access cases, for scenarios of interworking between EPC and 5GS and for scenarios of service exposure with EPC and 5GC interworking.

In both scenarios, an SCP (see also characteristic #2: service-based interfaces, communication and service mesh in clause 5.3), can be used for indirect communication between NFs and NF services within the VPLMN, within the HPLMN, or in within both VPLMN and HPLMN.

The network slicing feature is also applicable in roaming scenarios. In one aspect, ETSI TS 123 501 [i.2] specifies standard Slice/Service Types (SST) values for establishing global interoperability for network slicing so that even in roaming scenarios, support for most commonly used network slices, such as those related to Enhanced Mobile Broadband (eMBB), Ultra Reliable and Low Latency Communications (URLLC), Massive Internet of Things (MIoT) and Vehicle to Everything (V2X) services. In another aspect, the UE provides in the PDU session requests network slicing selection information both of the HPLMN and the VPLMN. In the case of VPLMN, such information is expected to be mapped to network slicing information selection of the HPLMN.

An additional aspect considered in the home routed roaming scenarios is the support of inter PLMN UP security (IPUPS) functionality set at the border of the respective VPLMN and HPLMN. The IPUPS is essentially a UPF that terminates the GTP-U tunnels over the N9 interface and deployed to increase the protection of the respective networks (see also characteristic #5: unified authentication framework in clause 5.6). Finally, as of 3GPP Release 16, roaming is not supported for Stand-alone Non-Public Networks (SNPN). In addition, ETSI TS 123 501 [i.2] notes that URLLC is not supported in home routed roaming scenario and that the interworking with edge computing is expected to only be applicable either in non-roaming cases or in local breakout roaming scenarios, i.e. UE is expected to access edge computing services which are close to the UE and thus delivered directly by the VPLMN.

5.9.2 Profiling of related NFV capabilities, features and specifications

5.9.2.1 General NFV concepts

The deployment of 5G systems with roaming capabilities is based on the actual deployment of respective HPMLN and VPLMN. Thus, the NFV capabilities documented in other characteristics analysis in the present document are the baseline for supporting also roaming scenarios. No additional NFV concepts and capabilities are thus referred.

The support of NS provisioning across multiple administrative domains specified in ETSI GS NFV-IFA 030 [i.27] might come close, conceptually, to roaming scenarios in respect to consider different administrative domains. The use cases of NS provisioning in multiple administrative domains focuses on the mechanisms by which an NS deployed in another administrative domain can be nested or used by the NFVO of another administrative domain. However, in the 5G system roaming scenarios, both HPLMN and VPLMN are in full control and managed by the respective network operators, hence there is no multiple administrative domain NS composition.

5.9.2.2 Specific profiling aspects and specification references

None to report.

5.9.3 Potential solutions

None to report. The present characteristic bases on the deployment of 5G system networks that respective home and visited network operators perform, and thus, of the solutions in other characteristics analysis documented in the present document.

5.9.4 Gap analysis

None to report.

5.10 Characteristic #9: Convergent (3GPP and non-3GPP) access

5.10.1 Introduction

5G design allows 5GC services to be available over multiple wireless access technologies like Wi-Fi™ or wired, besides 5G NR. The motivation is to exploit capabilities of multiple access networks to provide seamlessly high quality 5G services and optimize resource usage for the mobile network.

In scenarios where 5G RAN is not able to guarantee the intended service, for example in ultra-dense environments with poor 3GPP RAN coverage, and/or cases where there is extreme demand for high throughput, which cannot be covered or it can be covered but brings the 5GS operation to the limit, then using non-3GPP access and technologies like Wi-Fi™ can fill this gap. A number of interesting use cases and scenarios are described in the RAN Convergence Paper [i.28] like Enterprise Wi-Fi™ Convergence with 5G, Factories of the Future and In Home Wi-Fi™ Convergence with 5G.

According to ETSI TS 123 501 [i.2] the following types of non-3GPP access networks are defined:

1. Untrusted non-3GPP access networks

An untrusted non-3GPP access network can be connected to the 5G Core Network via a Non-3GPP InterWorking Function (N3IWF) (see figure 5.10.1-1). When the UE decides to use untrusted non-3GPP access to connect to a 5G CN, the UE first selects and connects with a non-3GPP access network; and it selects a PLMN and an N3IWF in this PLMN. User plane QoS differentiation between UE and N3IWF is supported as described in clause 5.7 of ETSI TS 123 502 [i.8].

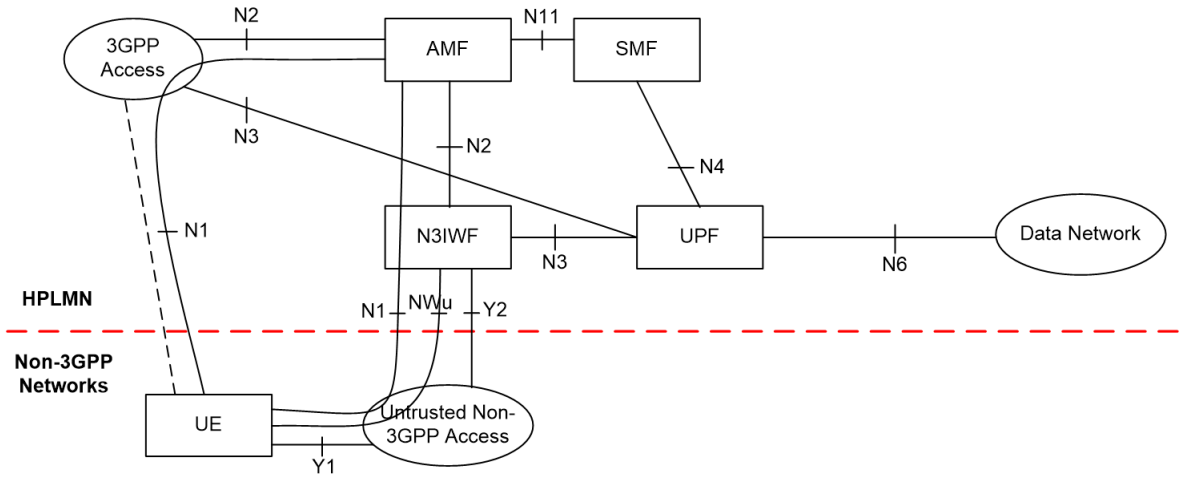


Figure 5.10.1-1: Non-roaming architecture for 5G Core Network with untrusted non-3GPP access (from ETSI TS 123 501 [i.2], figure 4.2.8.2.1-1)

Some primitive important procedures that are considered in this scenario are (not an exhaustive list):

- A UE that accesses the 5GC over a non-3GPP access, after UE registration, supports NAS signalling with 5GC control-plane functions using the N1 reference point.
- When a UE is connected via a NG-RAN and via a non-3GPP access, multiple N1 instances exist for the UE i.e. there is one N1 instance over NG-RAN and one N1 instance over non-3GPP access.
- A UE simultaneously connected to the same 5G CN of a PLMN over a 3GPP access and a non-3GPP access is served by a single AMF in this 5G CN.
- N3IWF supports the establishment of IPsec tunnels with the UE over NWu using IKEv2/IPsec.
- N3IWF is responsible for the selection of the appropriate AMF to serve the UE.

Although N3IWF is the successor of ePDG from 4G and they both serve as the gateway systems to offer non-3GPP access, they are fundamentally different. The main reason is that N3IWF is connected to AMF and UPF over N2 and N3 interfaces, which is also the case for a normal gNB.

In the control plane, N3IWF supports IPsec tunnel establishment with the UE for securing NAS messages, terminates N2 interface using NGAP and SCTP and also relays NAS signalling between AMF and UE.

In the user plane it terminates N3 interface using GTPU, relays both uplink and downlink user plane traffic and is responsible for the packet encapsulation/decapsulation of IPsec and GTPU tunnels. For uplink traffic for user packets received, N3IWF decapsulates the IPsec header and GRE header and encapsulate the UL PDU inside a GTPU packet with the appropriate QFI value to preserve QoS. The reverse operation (GTPU decapsulation and IPsec GRE encapsulation) is made to support downlink traffic send to UE over NWu.

Note that N3IWF supports the establishment of IPsec tunnels with the UE over NWu for UP and CP traffic. IPsec with ESP in tunnel mode as defined in IETF RFC 4303 [i.37] is expected to be configured, according to the process described in ETSI TS 133 501 [i.14], while authentication is based on Internet Key Exchange standard IKEv2 according to IETF RFC 7296 [i.38].

After IPsec establishment NAS signalling over N1 interface is initiated by N3IWF for the connection of the UE to AMF. The process is detailed in ETSI TS 133 501 [i.14] and ETSI TS 124 502 [i.35].

2. Trusted non-3GPP access networks

A trusted non-3GPP access network is connected to the 5G CN via a Trusted Non-3GPP Gateway Function (TNGF) (see figure 5.10.1-2). A non-3GPP access network can advertise the PLMNs for which it supports trusted connectivity and the type of supported trusted connectivity (e.g. "5G connectivity"). Therefore, the UEs can discover the non-3GPP access networks that can provide trusted connectivity to one or more PLMNs. When the UE decides to use trusted non-3GPP access to connect to a 5G CN in a PLMN: the UE first selects a PLMN; and then the UE selects a non-3GPP access network (a TNAN) that supports trusted connectivity to the selected PLMN. In this case, the non-3GPP access network selection is affected by the PLMN selection.

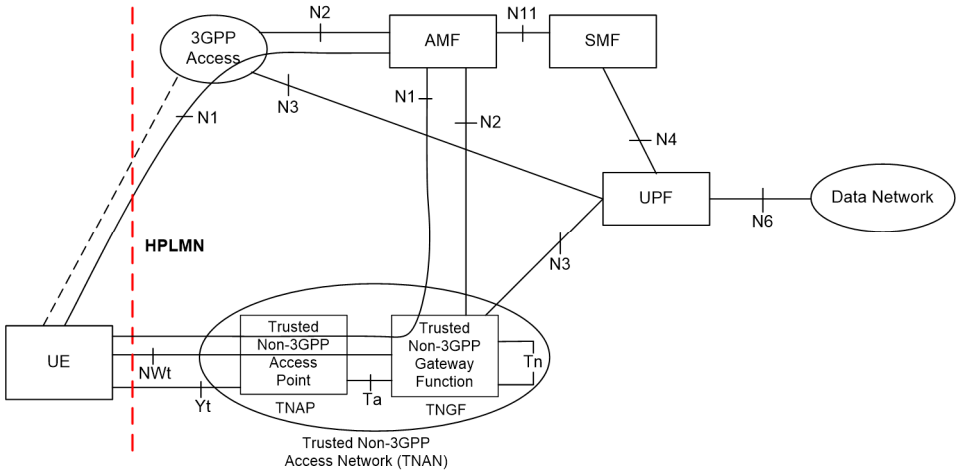


Figure 5.10.1-2: Non-roaming architecture for 5G Core Network with trusted non-3GPP access (from ETSI TS 123 501 [i.2], figure 4.2.8.2.1-2)

For both untrusted and trusted non-3GPP access, both the N3IWF and the TNGF interface with the 5G CN CP and UP functions via the N2 and N3 interfaces, respectively. Furthermore:

- A UE that accesses the 5G CN over a non-3GPP access, after UE registration, supports NAS signalling with 5G CN CP functions using the N1 reference point.
- A UE simultaneously connected to the same 5G Core Network of a PLMN over a 3GPP access and a non-3GPP access is served by a single AMF in this 5G Core Network.
- A UE establishes an IPsec tunnel with the N3IWF or with the TNGF to register with the 5G CN over non-3GPP access.
- User plane QoS differentiation between UE and N3IWF and between UE and TNGF is supported.

3. Wireline access networks

Wireline 5G Access Network (W-5GAN) can be connected to the 5G Core Network via a Wireline Access Gateway Function (W-AGF) (see figure 5.10.1-3). Like the previous cases, the W-AGF interfaces the 5G CN CP and UP functions via N2 and N3 interfaces, respectively. When a 5G-RG is connected via an NG-RAN and via a W-5GAN, there is one N1 instance over NG-RAN and one N1 instance over W-5GAN. A 5G-RG simultaneously connected to the same 5G CN of a PLMN over a 3GPP access and a W-5GAN access is served by a single AMF in this 5GC. 5G-RG maintains the NAS signalling connection with the AMF over the W-5GAN after all the PDU Sessions for the 5G-RG over that access have been released or handed over to 3GPP access. The 5G-RG connected to 5GC via NG-RAN is specified in ETSI TS 123 316 [i.29]. For the scenario of FN-RG, which is not 5G capable, connected via W-5GAN to 5GC, the W-AGF provides the N1 interface to AMF on behalf of the FN-RG.

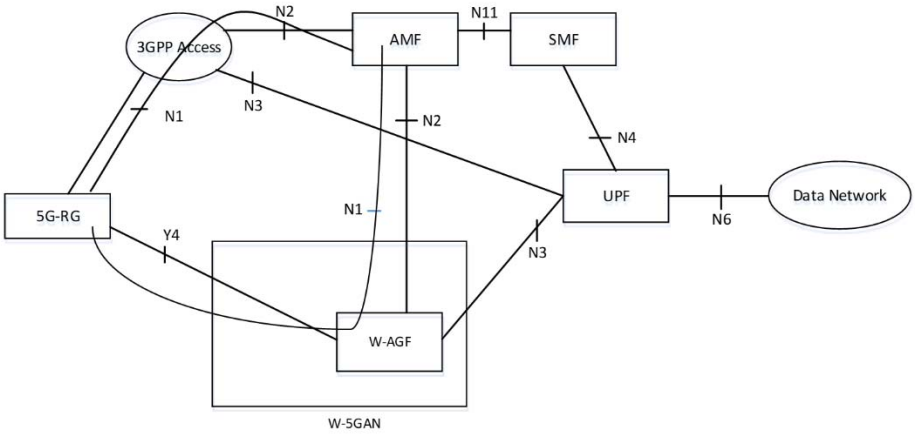


Figure 5.10.1-3: Non- roaming architecture for 5G Core Network for 5G-RG with Wireline 5G Access network and NG RAN ((from ETSI TS 123 501 [i.2], figure 4.2.8.4-1)

An important functionality introduced in 3GPP Release 16 is related to support for Access Traffic Steering, Switching and Splitting (ATSSS). ATSSS supports serving a PDU session over one or more concurrent accesses, i.e. 3GPP access, trusted non-3GPP access and untrusted non-3GPP access. After the establishment of a Multi-Access PDU Session, the UE applies network-provided policy (i.e. ATSSS rules) and considers local conditions (such as network interface availability, signal loss conditions, user preferences, etc.) for deciding how to distribute the uplink traffic across the two access networks. More information is provided in clause 5.32.6 of ETSI TS 123 501 [i.2].

5.10.2 Profiling of related NFV capabilities, features and specifications

5.10.2.1 General NFV concepts

The same general NFV concepts described in the characteristic Network capabilities exposure in clause 5.8 are applicable for the profiling of the present characteristic.

5.10.2.2 Specific profiling aspects and specification references

This clause focuses on the untrusted non-3GPP access case, and in particular on the N3IWF functionalities that are considered when deploying N3IWF as a VNF as part of an integrated 5G NS are elaborated.

In case N3IWF is deployed as a VNF, security management can follow ETSI GS NFV-SEC 013 [i.36] architecture like also the relevant security monitoring processes defined therein, for example for logs and traffic monitoring used to detect different types of attacks.

5.10.3 Potential solutions

5.10.3.1 Solution #9A: N3IWF deployed as a VNF/PNF

In this scenario, the N3IWF is deployed as a VNF (or PNF) and is part of single NSD describing an integrated 5GS NS. The integrated 5G NS covers the 5GC and the N3IWF functionality, exposed by the relevant NF instances. Through the NS SAP, untrusted non 3GPP Access networks like Wi-Fi™, can be connected to the 5GS and exploit 5GC services.

In principle N3IWF is considered a user plane function and the same virtualisation principles can be applied like in the case of gNB and UPF. To handle extensive packet processing and tunnelling operations, when being deployed as a VNF. For example, use of hardware acceleration to handle both the control plane and user plane pipelines used for access control, tunnel encapsulation and decapsulation and quality of service is considered. Functions like IPsec encryption and decryption and GTP encapsulation/decapsulation like also classification for thousands or even millions of flows can be extremely challenging to handle purely in software.

An N3IWF can be deployed as a VNF with a single VNFC instance or multiple VNFC instances for scalability. In addition, an N3IWF can also be deployed as a VNF with multiple VNFC types, e.g. one or two instances of a load balancer VNFC and multiple instances of another type of VNFC hosting the core functionality, which in turn can be instantiated multiple times for scalability.

Regarding N3IWF selection the N3IWF FQDN can be constructed using one of the following formats, as specified in clause 6.3.6 of ETSI TS 123 501 [i.2]: Operator Identifier based N3IWF FQDN; Tracking Area Identity based N3IWF FQDN; the N3IWF FQDN configured in the UE by the HPLMN. The N3IWF FQDN is used as input to the DNS mechanism for N3IWF selection according to ETSI TS 123 502 [i.8]. However, this is not foreseen to have a direct mapping to any NFV-MANO responsibility.

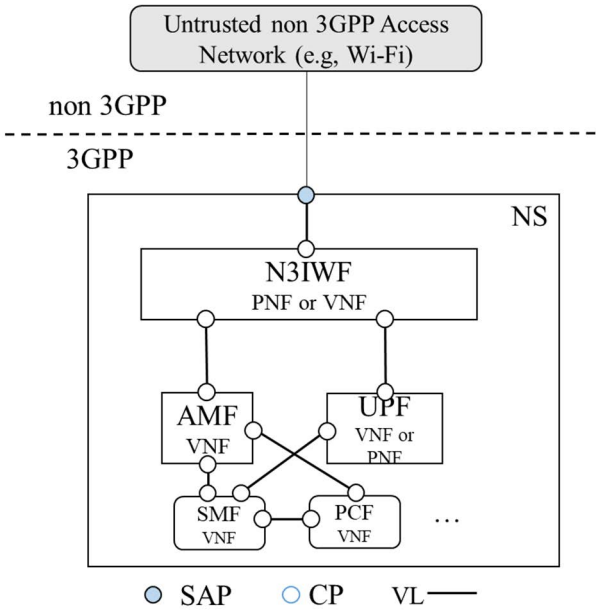


Figure 5.10.3.1-1: Single NS supporting all 5GS functionality and interfacing with untrusted non 3GPP access

5.10.3.2 Solution #9B: N3IWF deployed as an NS

In this scenario, the N3IWF is deployed as an independent NS, while also the 5GS is deployed as an integrated NS. A N3IWF NSD is used to describe the NS for deploying the N3IWF service where another NSD is used to describe the virtualised 5GS. Both are used by the NFVO to deploy the corresponding NS and perform the appropriate resource allocation. Like in the previous case N3IWF is considered as a user plane function and thus foreseen to maybe demand specific acceleration resources.

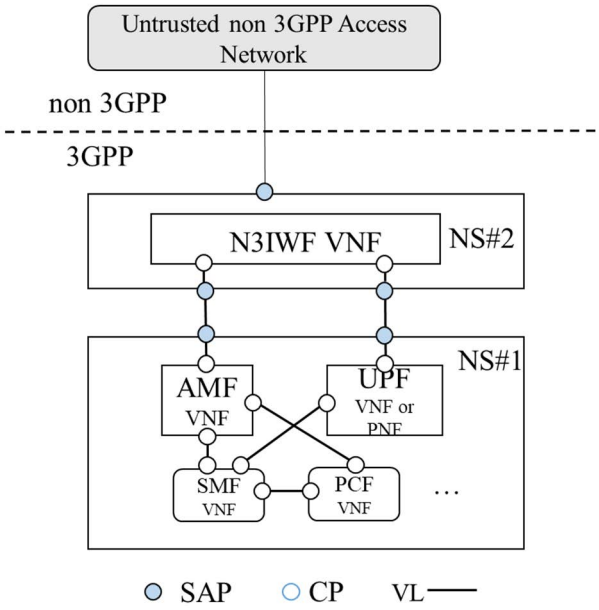


Figure 5.10.3.2-1: A NS supporting all 5GS functionality interfacing with a N3IWF service offering gateway functionality to connect untrusted non 3GPP access networks

5.10.4 Gap analysis

The referred ETSI NFV specifications in the present characteristic profiling do not document:

Gap #9.1: In case of network communication pre-provisioning between the non-3GPP access network and the N3IWF, Gap #3.1 also applies, as defined in characteristic #3 Network slicing (clause 5.4.4).

6 Recommendations

6.1 Overview

The present clause 6 documents recommendations about potential enhancements, changes, or clarifications to existing ETSI NFV specifications. The recommendations are derived based on the gap analysis performed on the profiling of NFV against the 5G characteristics documented in clause 5.

The recommendations are categorized and elaborated as follows:

- architecture and framework aspects (refer to clause 6.2);
- functional aspects (refer to clause 6.3);
- descriptors and other information/data model artefacts (refer to clause 6.4);
- interfaces and associated information/data model (refer to 6.5); and
- other recommendations, if any (refer to clause 6.6).

6.2 Recommendations related to the NFV architectural framework

The present clause provides recommendations focusing on enhancements to the NFV architectural framework, identifying potential new functions or functional blocks, and interactions among functional blocks.

Table 6.2-1 provides the recommendations related to the NFV architectural framework.

Table 6.2-1: Recommendations related to the NFV architectural framework

Identifier	Recommendation description	Comments and/or traceability
5gnfv.arch.001	It is recommended that a requirement be specified for the NFV architectural framework to support the inventory (a repository) of VNF Common and Dedicated Services and platform/infrastructure capabilities.	Refer to gap #2.2. This recommendation expects a repository where VNF Common/Dedicated Services, such as those used for service mesh, to be made available to existing NFV-MANO functional blocks, such as the VNFM and NFVO, so these functional blocks can know the supported capabilities and refer to those services when performing the NS, VNF and virtualised resources LCM. Refer also to clause 8.2 of ETSI GR NFV-IFA 029 [i.16] regarding "PaaS related use cases" and the definition of generic VNF Common/Dedicated Services.
5gnfv.arch.002	It is recommended that a requirement be specified for the NFV architectural framework to support operator certificate management functions for the different certificate categories related to VNF and VNFC instances. The new certificate management functions communicate with VNFM and the NFVO for purposes of synchronizing LCM operations for certificates with VNF/VNFC LCM.	Refer to gap #5.5.

6.3 Recommendations related to functional aspects

The present clause provides recommendations focusing on functional aspects of the functional blocks of the NFV architectural framework.

Table 6.3-1 provides the recommendations related to functional aspects.

Table 6.3-1: Recommendations related to functional aspects

Identifier	Recommendation description	Comments and/or traceability
5gnfv.func.001	It is recommended that a requirement be specified for the VNFM to support adding/removing VNF external CP that are not sub-ports of a trunk.	Refer to gap #7.2. This recommendation extends current functionality of the VNFM to add/remove VNF external CP which are sub-ports of a trunk to other types of VNF external CP.

Identifier	Recommendation description	Comments and/or traceability
5gnfv.func.002	It is recommended that a requirement be specified for the VNFM to support determining if a managed VNF will use VNF Common/Dedicated Services and request to the "PaaS services management function" to allocate such a service.	Refer to gap #2.2. The VNFM is expected to be able to refer to VNF Common/Dedicated Services that are to be used by the VNF. Because ETSI GR NFV-IFA 029 [i.16] does not conclude on a specific solution for the mapping of the PaaS services management, a generic "PaaS services management function" term is used in the recommendation. Determining the mapping and architectural option of "PaaS service management function" is out of the scope of the present document.
5gnfv.func.003	It is recommended that a requirement be specified for the NFVO to support determining if a managed VNF will use VNF Common/Dedicated Services and request to the "PaaS services management function" to allocate such a service.	Refer to gap #2.2. The NFVO is expected to be able to refer to VNF Common/Dedicated Services as part of the resource orchestration and preparation of CIS cluster/NFVI capabilities for the subsequent deployment of VNF and NS constituents. Because ETSI GR NFV-IFA 029 [i.16] does not conclude on a specific solution for the mapping of the PaaS services management, a generic "PaaS services management function" term is used in the recommendation. Determining the mapping and architectural option of "PaaS service management function" is out of the scope of the present document.
5gnfv.func.004a	It is recommended that requirements are specified to allow onboarding of an NSD even if not all the VNF Packages providing the VNFDs referred in the NSD, as well as nested NSDs and PNFDs, have previously been on-boarded to the NFVO.	Refer to gap #1.2. The NFVO is expected to support NSD file archives provided by NS designers that include VNFs that deploy different 5G NF services.
5gnfv.func.004b	It is recommended that requirements are specified for the NFVO to support processing information related to the version dependencies between constituent VNFs in an NS.	Refer to gap #1.3. It is expected to further evaluate issues of version dependencies in case of NS being used to assemble set of NF services.
5gnfv.func.005	It is recommended that a requirement be specified for the NFVO to support requesting to the VNFM the modification of security group of a particular VNF instance that uses security group (as defined in the VNFD) when a destination CP of the VNF instance is being added/removed during the LCM of the corresponding VNF instance.	Refer to gap #5.1. This recommendation extends current functionality of security group to be able to modify the rule.

Identifier	Recommendation description	Comments and/or traceability
5gnfv.func.006	It is recommended that a requirement be specified for the NFVO to support requesting to the VNFM to register/unregister client information with the respective authorization server when client credential of corresponding VNF instance are being added/removed during the LCM of the corresponding VNF instance.	Refer to gaps #5.2 and #5.4. The NFVO is expected to be able to refer to VNF Common/Dedicated Services as part of the network orchestration and preparation of authorization when the authorization server is implemented as VNF Common or Dedicated Service.
5gnfv.func.007	It is recommended to update the definition of VNF in ETSI GR NFV 003 [i.1] to clarify that a VNF can be used to deploy the implementation of a subset of an NF, as long as the behaviour and interfaces of this NF subset are well defined.	Refer to gap #1.1, gap#1.2, gap#1.3.
5gnfv.func.008	It is recommended that a requirement be specified for the new certificate management functions to synchronize the LCM of the certificates required by the VNF/VNFC with the LCM operations of the VNF/VNFC. The certificate management functions keep track of the associated certificates with each of the VNF/VNFC instances and are able to query runtime information for those VNF/VNFCs.	Refer to gaps #5.5.

6.4 Recommendations related to NFV descriptors and other artefacts

The present clause provides recommendations focusing on NFV descriptors, packaging and other artefacts.

Table 6.4-1 provides the recommendations related to NFV descriptors, packaging and other artefacts.

Table 6.4-1: Recommendations related to NFV descriptors and other artefacts

Identifier	Recommendation description	Comments and/or traceability
5gnfv.desc.001	It is recommended that a requirement be specified for the VNFD and NSD to support describing requirements to use VNF Common/Dedicated Services related to service mesh provided by the infrastructure or platform.	Refer to gap #2.1 and gap #2.2.
5gnfv.desc.002	It is recommended that a requirement be specified for the NSD to support specifying capabilities to be offered by the VL regarding services such as name resolution, communication security and load-balancing for specified connection points.	Refer to gap #2.3.
5gnfv.desc.003	It is recommended that a requirement be specified for the VNFD to support defining scaling aspects in which virtualised storage resources of the VNF can be scaled independently or together with other VNF constituents.	Refer to gap #6.1.
5gnfv.desc.004	It is recommended that a requirement be specified for the VNFD to support defining whether the VNF can use shared virtualised storage resources.	Refer to gap #6.2.
5gnfv.desc.005	It is recommended that a requirement be specified for the NSD to support defining what VNFs are expected to use virtualised storage resources to be shared among VNFs.	Refer to gap #6.2.
5gnfv.desc.006	It is recommended that a requirement be specified for the VNFD to support defining in the CP descriptors network service properties above L3.	Refer to gap #7.3. Network service properties above L3 are expected to include: transport layer ports and protocols.

Identifier	Recommendation description	Comments and/or traceability
5gnfv.desc.007a	It is recommended that requirements are specified for the NSD and NSD file archive to include an indication if the onboarding of an NSD can be performed even if not all the VNF Packages providing the VNFDs, or nested NSDs, or PNFDs, referred in the NSD, have previously been on-boarded to the NFVO.	Refer to gap #1.1. The NSD and the NSD file archives can be provided by NS designers and include VNFs that deploy different 5G NF services. See also 5gnfv.func.004a.
5gnfv.desc.007b	It is recommended that requirements are specified for the NSD and/or NSD file archive to support information related to the version dependencies between constituent VNFDs in the NSD.	Refer to gap #1.3. See also 5gnfv.func.004b.
5gnfv.desc.008	It is recommended that a requirement be specified for the NSD to support defining as part of the NS profile the mapping of a CP that uses security group to target CP.	Refer to gap #5.1.
5gnfv.desc.009	It is recommended that a requirement be specified for the VNFD to support describing requirements to use VNF Common/Dedicated Services related to authorization server provided by the infrastructure or platform.	Refer to gap #5.2.
5gnfv.desc.010	It is recommended that a requirement be specified for the VNFD to support describing requirements to use VNF Common/Dedicated Services related to CA provided by the infrastructure or platform.	Refer to gap #5.3. To realize certificate distribution described in ETSI GR NFV-SEC 005 [i.34].
5gnfv.desc.011	It is recommended that a requirement be specified for the VNFD to enable identifying if a VNF provides authorization server capabilities.	Refer to gap #5.2.

6.5 Recommendations related to interfaces and information model

The present clause provides recommendations focusing on interfaces and associated information.

Table 6.5-1 provides the recommendations related to NFV descriptors, packaging and other artefacts.

Table 6.5-1: Recommendations related to interfaces and information model

Identifier	Recommendation description	Comments and/or traceability
5gnfv.if.001	It is recommended that a requirement be specified for the NS LCM interface produced by the NFVO to support providing information about external L2 networks where the NS constituents are expected to be connected via the exposed SAP.	Refer to gap #3.1. Such information is expected to be provided during NS LCM operations of NS instantiation and NS update.
5gnfv.if.002	It is recommended that a requirement be specified for the NS LCM interface produced by the NFVO to support providing location constraints of constituents of a VNF to be deployed.	Refer to gap #4.1.
5gnfv.if.003	It is recommended that a requirement be specified for the NS LCM interface produced by the NFVO to support providing naming related information (e.g. FQDN) associated to the SAP or VNF external CP.	Refer to gap #7.3, gap #2.3.
5gnfv.if.004	It is recommended that a requirement be specified for the VNF LCM interface produced by the VNFM to support adding/removing VNF external CP that are not sub-ports of a trunk.	Refer to gap #7.2. This recommendation extends current functionality of the VNFM to add/remove VNF external CP which are sub-ports of a trunk to other types of VNF external CP.

Identifier	Recommendation description	Comments and/or traceability
5gnfv.if.005	It is recommended that a requirement be specified for the VNF Lifecycle Operation Granting interface produced by the NFVO to support granting the use of already created virtualised resources.	Refer to gap #6.2. This recommendation will support the sharing of virtualised storage resources, i.e. the NFVO can indicate back to the VNFM to reuse an existing resource instead of creating a new one.
5gnfv.if.006	It is recommended to relax the requirements on NSD onboarding to allow NSD onboarding when not all the VNF packages providing the constituent VNFDs, or the nested NSDs or PNFDs, have previously been onboarded. The NS LCM is updated to only check for the onboarded VNF packages that contain the VNFDs, or for onboarded nested NSDs, that are required in the deployment flavour used for the respective NS LCM operation.	Refer to gap #1.2. The NFVO is expected to support onboarding NSD file archives provided by NS designers that include VNFs that deploy different 5G NF services, and to support any associated impacts to the NSD onboarding and NS LCM. See also 5gnfv.func.004a.
5gnfv.if.007	It is recommended that a requirement be specified for the VNF LCM interface produced by the VNFM to support modifying security groups.	Refer to gap #5.1 This recommendation is aimed to support 5gnfv.func.005.
5gnfv.if.008	It is recommended that a requirement be specified for the VNF LCM interface produced by the VNFM to support modifying managed information on a particular VNF related to specific types of VNF Common/Dedicated Services used by this VNF.	Refer to gaps #5.2 and #5.4. This recommendation is aimed to support 5gnfv.func.006, 5gnfv.if.009 and 5gnfv.if.010. Specific types of VNF Common/Dedicated Services can be those providing "authorization server" capabilities, and the VNF LCM interfaces enables setting and modifying information for those types of services.
5gnfv.if.009	It is recommended that a requirement be specified for the VNF Configuration interface produced by the VNF to support modifying managed information on a particular VNF related to one or more specific types of VNF Common/Dedicated Services used by this VNF.	Refer to gap #5.4. This recommendation is aimed to support 5gnfv.func.006 and 5gnfv.if.008.
5gnfv.if.010	It is recommended that a requirement be specified for the VNF Configuration interface produced by the VNF to support the capability to configure information related to the clients to authorize when the VNF acts as authorization server.	Refer to gap #5.4. This recommendation is aimed to support 5gnfv.func.006 and 5gnfv.if.008.
5gnfv.if.011	It is recommended that requirements be specified for the certificate management functions to support retrieval from the VNFM and NFVO of VNF/VNFC runtime information and VNF/VNFC LCM events.	Refer to gap #5.5.

6.6 Other recommendations

The present clause provides other recommendations to specifically related to other categories of foreseen enhancements of NFV.

Table 6.6-1 provides other recommendations.

Table 6.6-1: Other recommendations

Identifier	Recommendation description	Comments and/or traceability
5gnfv.other.001	It is recommended to document potential use of non-MANO artefacts describing the relationship of scaling aspects with the purposed services offered by the VNF.	Refer to gap #1.1. The means and what non-MANO artefacts are known to a consumer is via the "non-MANO artefacts registry"; therefore, the recommendation could be addressed by defining the appropriate registry entries.

7 Conclusion

The present document studies 5G characteristics and profiles the NFV architectural framework and its capabilities for the deployment of 5G systems. Potential solutions on how to leverage NFV capabilities or extend them are described and potential technical gaps of NFV are identified. Recommendations for additional normative work relevant to the scope of the present document are derived.

The set of recommendations indicate the need to perform additional normative specification work to enhance the capabilities of the NFV architectural framework to better support the deployment of 5G system. The aspects for which additional normative work are identified are:

- Recommendations related to NFV architectural aspects (refer to clause 6.2).
- Recommendations related to functional aspects of the NFV architectural framework and its functional blocks (refer to clause 6.3).
- Recommendations related to NFV descriptors and other artefacts (refer to clause 6.4).
- Recommendations related to interfaces and associated information models (refer to clause 6.5).

Annex A:
Change History

Date	Version	Information about changes
November 2019	0.0.1	Implementation of contributions approved at IFA#171-F2F_Leganes-Madrid: - NFVIFA(19)000900, NFVSOL(19)000901. Rapporteur action: delete the authors annex.
January 2020	0.1.0	Implementation of contributions approved at IFA#181: - NFVIFA(19)0001021: IFA037 Clause 4.1 Introduction to 5G network, - NFVSOL(19)0001022: IFA037 Clause 4.2 Characteristics of 5G network.
January 2021	0.2.0	Implementation of contributions approved at IFA#220: - NFVIFA(20)000830: IFA037 Clause 5.1 Introduction to characteristics, - NFVIFA(20)000760r1: IFA037 Clause 5 Adding characteristic NF modularization
March 2021	0.3.0	Implementation of contributions approved at IFA#228: - NFVIFA(21)000100r1: FEAT21 IFA037 Clause 5 Adding characteristic SBI, communication and service mesh - NFVIFA(21)000099r3: FEAT21 IFA037 Clause 5 Adding characteristic network slicing
May 2021	0.4.0	Implementation of contributions approved at IFA#235: - NFVIFA(21)000293r1: FEAT21 IFA037 Clause 5 Adding characteristic distribution of services across the network - NFVIFA(21)000329r1: IFA037 Clause 5 Adding characteristic Unified authentication framework Additional rapporteur changes: - Updated the reference numbers in text of existing reference documentation present in clause 2.2. - Corrected the numbering of various solutions in clause 5.6.3.
June 2021	0.5.0	Implementation of contributions approved at IFA#234; - NFVIFA(21)000257: IFA037 Clause 5 Adding characteristic Stateless NF Implementation of contributions approved at IFA#242: - NFVIFA(21)000496r1: FEAT21 IFA037 5.6 Adding potential solutions for characteristic Unified authentication framework - NFVIFA(21)000502: FEAT21 IFA037 Clause 5 Adding characteristic Network capabilities exposure - NFVIFA(21)000526: FEAT21 IFA037 Clause 5 Adding characteristic roaming Additional rapporteur changes: - Clause 5.5.3.4: Corrected styles in first two paragraphs. - Implementation of 257: corrected wrong references to 23.501 and added abbreviations in clause 3.3 of several abbreviations used in the contribution. Changed type and font of all figures to use Times New Roman, for consistency with other figures in the document. - Implementation of 496r1: added missing references to IFA006, IFA008 and IETF RFC 6749. Changed type and font of all figures to use Times New Roman, for consistency with other figures in the document. - Implementation of 502: Changed type and font of all figures to use Times New Roman, for consistency with other figures in the document.
June 2021	0.6.0	Implementation of contributions approved at IFA#243: - NFVIFA(21)000522r1: FEAT21 IFA037 Clause 5 Adding characteristic Convergent (3GPP and non-3GPP) access - NFVIFA(21)000543: FEAT21 IFA037 Start cleaning up EN - NFVIFA(21)000545: FEAT21 IFA037 Clause 5.4 Completing solutions of network slicing Additional rapporteur changes: - Implementation of 522r1: added new reference [i.29], clause 5.10.2.2, corrected wrong reference to TS 23.502; clause 5.10.2.1, provided the correct clause number as per the "Rapporteur's Note" action. - Implementation of 543: Addressed rapporteur's note in clause 5.1 - Implementation of 545: references to IFA006 and IFA030 not needed because they were already part of the informative references list.

Date	Version	Information about changes
July 2021	0.7.0	Implementation of contributions approved at IFA#244: - NFVIFA(21)000544: FEAT21 IFA037 Clause 5.3 Adding missing solutions on SBI, communication and mesh - NFVIFA(21)000573: FEAT21 IFA037 Clause 5.2 Gap analysis modularization - NFVIFA(21)000574: FEAT21 IFA037 Clause 5.3 Gap analysis SBI - NFVIFA(21)000575: FEAT21 IFA037 Clause 5.4 Gap analysis network slicing - NFVIFA(21)000576r1: FEAT21 IFA037 Clause 5.4 Gap analysis services distribution
July 2021	0.8.0	Implementation of contributions approved at IFA#245: - NFVIFA(21)000592r1: FEAT21 IFA037 Clause 5.7 Gap analysis stateless NF - NFVIFA(21)000593: FEAT21 IFA037 Clause 5.9 cleaning up editor notes - NFVIFA(21)000594: FEAT21 IFA037 Clause 5.10 Gap analysis convergent access
July 2021	0.9.0	Implementation of contributions approved at IFA#246: - NFVIFA(21)000595r2: FEAT21 IFA037 Clause 5.8 Gap analysis Network capabilities exposure - NFVIFA(21)000639r1: FEAT21 IFA037 Clause 6.1 Adding recommendations overview - NFVIFA(21)000660: FEAT21 IFA037 Clause 7 Adding Conclusion
July 2021	0.10.0	Implementation of contributions approved at IFA#248: - NFVIFA(21)000659r2: FEAT21 IFA037 Clause 6 Adding recommendations related to all characteristics
August 2021	0.11.0	Implementation of contributions approved at IFA#249 and approved at IFA#251: - NFVIFA(21)000677r2: FEAT21 IFA037 Clause 5.6 addresses Editor's Note about SEC005 and gap analysis of unified authentication framework - NFVIFA(21)000678r4: FEAT21 IFA037 Clause 6 Adding recommendations related to unified authentication - NFVIFA(21)000698: FEAT21 IFA037 Clauses 5.4.2.2 and 6.5 addressing EN about L2 connectivity - NFVIFA(21)000722r3: FEAT21 IFA037 Start cleaning up EN_nef_non3gpp Additional rapporteur changes: - Add informative references to IETF RFC 4303 and IETF RFC 7296 introduced by content in the NFVIFA(21)000722r3.
September 2021	0.11.1	Implementation of contribution approved at IFA#252 and IFA#253: - NFVIFA(21)000748r1: IFA037 Review clause 1,3,4 editorial clean-up - NFVIFA(21)000749r1: IFA037 Review clause 5 editorial clean-up - NFVIFA(21)000768r1: IFA037 Review clause 6 editorial clean-up Additional rapporteur changes: - Remove multiple consecutive spaces (e.g. double spaces). - Further alignment of /s/artifact/artefact. - Harmonization: use "Solution" (with capital letter) when naming/referring a specific solution. - Harmonization: use "figure" when referencing to a figure, instead of "Figure" (with capital F). - Some typos corrected.

Date	Version	Information about changes
October 2021	0.12.0	Implementation of contributions approved/agreed at IFA#254, IFA#255 and IFA#256: - NFVIFA(21)000796r1: IFA037 review - editorial fixes and small technical wording improvements - NFVIFA(21)000798r2: IFA037 review - miscellaneous technical improvements - NFVIFA(21)000809r1: FEAT21 IFA037 Clause 4 to 5.6.2.2 Minor miscellaneous changes - NFVIFA(21)000820r1: FEAT21 IFA037 Clauses 5.7 to 5.10 Miscellaneous changes - NFVIFA(21)000821r1: FEAT21 IFA037 Clauses 6 Miscellaneous changes to recommendations - NFVIFA(21)000822: FEAT21 IFA037 Deleting unused clauses - NFVIFA(21)000807: FEAT21 IFA037 Clause 5.1 Statement of 3GPP Release baseline and update of references - NFVIFA(21)000842r2: FEAT21 IFA037 Remaining miscellaneous changes from 797 comments - NFVIFA(21)000849: FEAT21 IFA037 Clause 5.6 Clarifying security aspects - NFVIFA(21)000848r2: FEAT21 IFA037 adding missing gap and recommendations - NFVIFA(21)000852: FEAT21 IFA037 proposed updates - security review clause 5.6 - NFVIFA(21)000872r1: FEAT21 IFA037 security recommendations gap 5.5 Additional rapporteur changes: - Additional alignment of terminology of "VNF Common/Dedicated Services" done following the guidelines from contribution NFVIFA(21)000821r1. - Implementation of 848r2: minor corrections in the recommendations numbering and correct the reference in the 5gnfv.if.006 to point to gap #1.2. - Implementation of 842r2: Figure 5.3.3.3.3-1: additional change of "CaaS" to be replaced by "CIS cluster". - Figure 5.10.3.1-1 and 5.10.3.2-1: changed the fonts to Times New Roman, to align styles with other edited figures. In addition, corrected the figure numbering. - Figure 5.6.1-3: changed the text edited figure and pasted a copy from the IETF RFC 6749 as png. - Minor editorial/typo errors fixed and applied some ETSI styles. - Clause 5.8.4: added the following sentence for consistency with other "Gap analysis" clauses: "The referred ETSI NFV specifications in the present characteristic profiling do not document:" - Table 6.4-1: corrected the recommendation number of 5gnfv.desc.012 → 011.

History

Document history		
V4.1.1	December 2021	Publication